

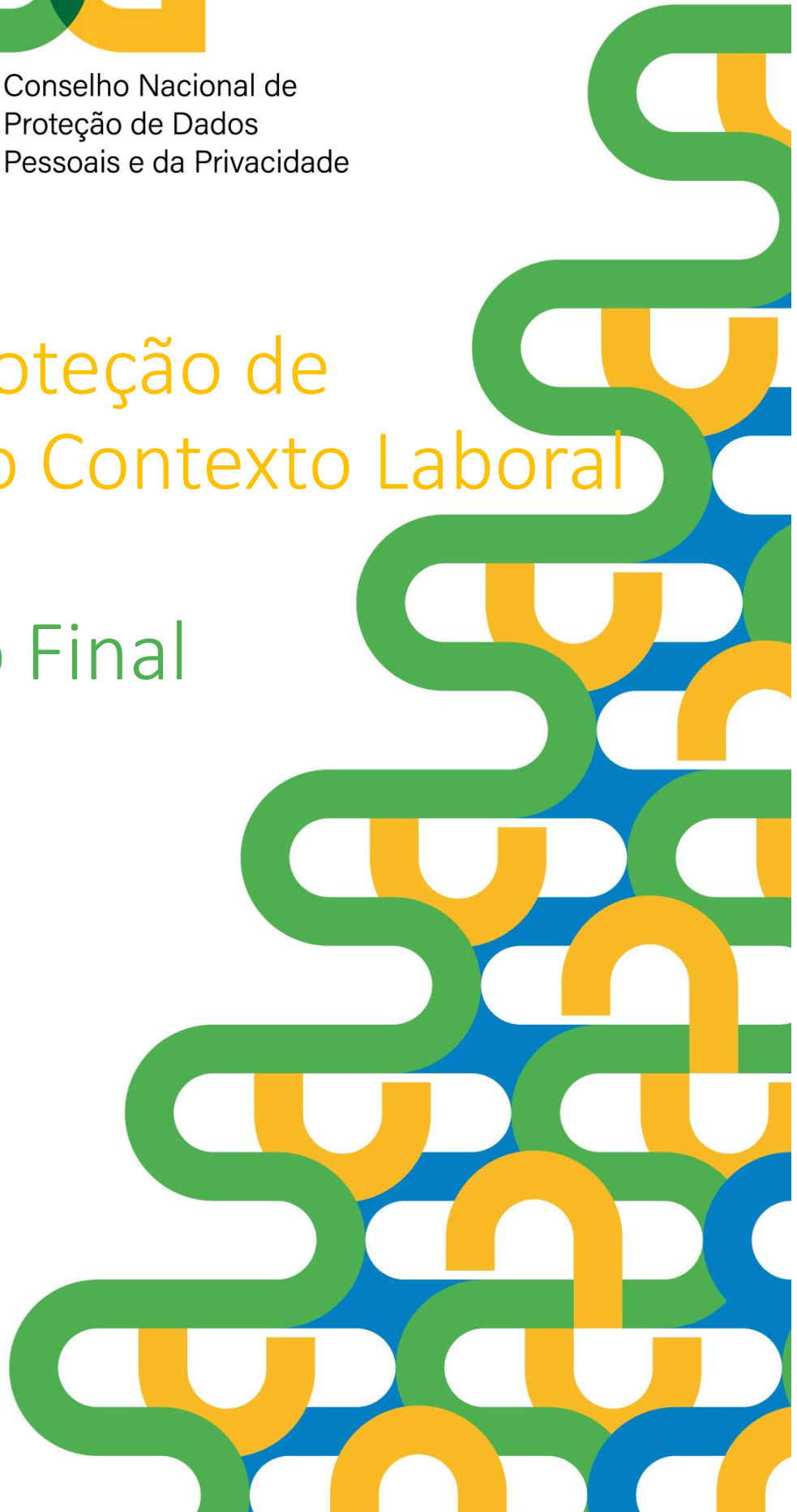


Conselho Nacional de  
Proteção de Dados  
Pessoais e da Privacidade

# GT1 – Proteção de Dados no Contexto Laboral

## Relatório Final

# 2026





## **Conselheiros Membros:**

### **Débora Sirotheau Siqueira Rodrigues**

membro titular representante de entidades representativas do Setor Laboral  
(coordenadora)

### **Alexandre Zago Boava**

membro titular representante de entidades representativas do Setor Laboral (vice  
coordenador)

### **Cassio Augusto Muniz Borges**

membro titular representante de Confederações Sindicais das categorias  
econômicas do setor produtivo;

### **Isabella Vieira Machado Henriques**

membro titular representante de Organizações da Sociedade Civil com atuação  
comprovada em proteção de dados pessoais; e

### **João Marcos Pereira Vidal**

membro suplente representante de entidades representativas do Setor Laboral.

## SUMÁRIO

Agradecimentos Especiais .....	3
2. Metodologia .....	5
3. Histórico das Atividades Desenvolvidas .....	6
4. Contextualização: elementos estruturantes da proteção de dados no contexto laboral	6
4.1 Atores no tratamento de dados no contexto laboral .....	7
4.2 Assimetria estrutural das relações de trabalho .....	9
4.3. Ciclo de vida dos dados no Contexto Laboral .....	9
4.4. Economia Digital, datificação e plataformização .....	10
4.5 Infraestrutura digital e dependência tecnológica .....	11
4.6 Estrutura analítica do relatório .....	11
5. Princípios e Hipóteses Legais no Tratamento de Dados Pessoais no Contexto Laboral	11
6. Transparência e Exercício de Direitos dos Titulares .....	15
7. Tecnologias de monitoramento e produtividade .....	20
7.1 Proporcionalidade e limitação à finalidade .....	21
7.2 Parâmetros éticos e técnicos para biometria, geolocalização, câmeras e softwares de produtividade .....	21
7.3 Transparência sobre algoritmos de pontuação e ranqueamento .....	23
7.4 Riscos discriminatórios diretos e indiretos .....	25
7.5 Questões específicas dos trabalhadores plataformizados.....	26
7.5.1. Situações de especial vulnerabilidade: crianças e adolescentes em plataformas digitais.....	26
8. Diálogo social e negociação coletiva no contexto da proteção de dados laboral .....	29
8.1 Fundamento jurídico da negociação coletiva no ordenamento brasileiro e internacional .....	30
8.2 Transparência coletiva e transparência algorítmica .....	30
8.3 Desafios para a efetividade da negociação coletiva no Brasil .....	33
9. Parecer Conclusivo e Subsídios Propostos.....	35
9.1. Diagnóstico do Cenário Atual.....	35
9.2. Convergências e Tensões Identificadas .....	38
9.3. Propostas de abordagens .....	39
10. Conclusão.....	46
11. Anexos.....	48

## **Agradecimentos Especiais**

O Grupo de Trabalho nº 1 (GT1) do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd) expressa seus mais sinceros agradecimentos a todas as pessoas e instituições que, por meio de entrevistas, envio de materiais, contribuições técnicas e compartilhamento de experiências, tornaram possível a elaboração deste relatório final sobre “Proteção de dados pessoais no contexto laboral”.

A riqueza e a profundidade das análises aqui consolidadas são fruto direto da generosidade intelectual e do compromisso com o debate público demonstrados por cada um dos especialistas e instituições participantes. Em especial, agradecemos:

- **Albert Franca Josua Costa**
- **Ana Rita Biba de Almeida**
- **Caroline de Melo Lima Gularte**
- **Carolina Tupinambá**
- **Carlos Fernandes Coninck Júnior**
- **Emerson Wallace**
- **Gaudio Ribeiro de Paula**
- **Helena Dominguez Paes Landim Bianchi**
- **Iagê Miola**
- **Jorge André Ferreira Fontelles de Lima**
- **Luciana Freire**
- **Martha Leal**
- **Pedro Saliba**
- **Priscila Zoghbi**
- **Rafael Mosele**
- **Renan Bernardi Kalil**
- **Rodrigo Santana dos Santos**
- **Rony Vainzof**

- **Roseli Aparecida Figaro Paulino**
- **Selma Carloto**
- **Tatiana Bhering Roxo**
- **Tayná Araújo**
- **Thamara Consul Gavazza**
- **Volia Bomfim**
- **Agência Nacional de Proteção de Dados - ANPD**
- **Confederação Nacional da Indústria - CNI**
- **Central Única dos Trabalhadores - CUT**
- **Data Privacy Brasil**
- **Federação das Indústrias do Estado do Rio de Janeiro - FIRJAN**
- **Federação das Indústrias do Estado de São Paulo - FIESP**
- **Instituto Nacional de Proteção de Dados – INPD**
- **Instituto ALANA**
- **Opice Blum Bruno Advogados Associados**
- **Serviço Federal de Processamento de Dados - SERPRO**

A todos, o nosso reconhecimento e gratidão. Este relatório é, antes de tudo, uma construção coletiva.

## 1. Introdução

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPd), no exercício de suas atribuições consultivas e propositivas, instituiu, por meio da **Portaria CNPD nº 01, de 05 de novembro de 2025**, o **Grupo de Trabalho (GT) dedicado à temática da Proteção de Dados no Contexto Laboral**. Este GT foi criado com a missão de realizar análises, estudos e elaborar proposições que contribuam para o equilíbrio entre a proteção da privacidade e dos dados pessoais dos trabalhadores e as legítimas necessidades operacionais, de segurança e de gestão das organizações, em conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018)**.

A relação laboral contemporânea é cada vez mais mediada por tecnologias que implicam no tratamento massivo de dados pessoais – desde informações cadastrais e biométricas até dados de monitoramento de desempenho, localização, comunicações e saúde. Essa realidade, embora traga ganhos de eficiência e segurança, também suscita desafios complexos para a garantia do direito fundamental à privacidade e à proteção de dados pessoais, que são o fundamento da autodeterminação informacional.

Neste cenário, a atuação deste Grupo de Trabalho se mostrou não apenas oportuna, mas estratégica. O GT reuniu-se ao longo de **cento e vinte dias**, realizando **reuniões ordinárias** e conduzindo **entrevistas com especialistas e representantes** da academia, órgãos públicos, setor empresarial, organizações da sociedade civil e representantes sindicais. Esses diálogos multissetoriais permitiram um diagnóstico abrangente e plural dos principais pontos de atenção, práticas existentes e lacunas regulatórias na interface entre o direito à proteção de dados e o mundo do trabalho.

O presente **Relatório Final** consolida os trabalhos realizados, apresentando o histórico das atividades, os produtos elaborados e, sobretudo, um **parecer conclusivo com subsídios técnicos e proposições concretas**. O documento tem como objetivo primordial oferecer ao CNPD e à Agência Nacional de Proteção de Dados (ANPD) insumos fundamentados para a futura elaboração de orientações, normativos ou políticas públicas que promovam um ambiente laboral digitalmente ético, seguro e em plena conformidade com o ordenamento jurídico de proteção de dados pessoais no Brasil.

A seguir, são detalhadas as atividades desenvolvidas, as conclusões alcançadas e as recomendações propostas.

## 2. Metodologia

O Grupo de Trabalho adotou uma metodologia qualitativa, colaborativa e multissetorial, estruturada para garantir a abrangência, profundidade e legitimidade das suas análises e proposições. Os trabalhos foram conduzidos em três etapas principais:

### 2.1. Fase de Planejamento e Fundamentação

- Aprovação do plano de trabalho, conforme Art. 4º da Portaria CNPD nº 01/2025.
- Definição dos eixos temáticos centrais a serem investigados.

### 2.2. Fase de Coleta de Dados e Subsídios

- Reuniões Ordinárias do Colegiado: Realização reuniões técnicas, sempre às segundas-feiras, com pauta predefinida e discussões registradas em atas, conforme previsto nos Arts. 5º e seguintes da Portaria.
- Ciclo de Entrevistas e Audiências Técnicas: Condução de entrevistas com especialistas acadêmicos, representantes de entidades do setor empresarial, sindicatos laborais, organizações da sociedade civil e profissionais da área jurídica e de compliance. Cada entrevista foi registrada em ata específica, documentando os pontos de vista e contribuições recebidas.
- Análise de Contribuições Escritas: Consideração de materiais, estudos e posicionamentos enviados pelos especialistas e entidades contatadas.

### **2.3. Fase de Análise e Síntese**

- Sistematização e análise crítica de todas as informações coletadas.
- Discussões coletivas no âmbito do GT para identificar convergências, divergências e pontos sensíveis.
- Elaboração deste relatório, com revisões internas até a consolidação final.

Esta abordagem permitiu um exame multidimensional do tema, alinhando fundamentação teórica e percepções práticas dos atores envolvidos.

## **3. Histórico das Atividades Desenvolvidas**

As seguintes atividades foram executadas pelo GT1:

### **3.1. Reuniões Ordinárias Realizadas**

Lista das reuniões realizadas, com data, participantes e principais temas deliberados.

### **3.2. Entrevistas e Audiências com Especialistas e Entidades**

Relação das entrevistas realizadas, com:

- Nome da entidade ou especialista;
- Data da entrevista;
- Principais contribuições para o GT.

### **3.3. Elaboração de Documentos Internos do GT**

- Atas de reunião;
- Eixos temáticos;
- Compilação de contribuições dos especialistas entrevistados.

### **3.4. Subsídios Técnicos Produzidos**

- Diagnóstico de desafios na aplicação da LGPD no ambiente laboral;
- Proposta de tópicos para diretrizes ou normativos da ANPD.

## 4. Contextualização: elementos estruturantes da proteção de dados no contexto laboral

A análise das contribuições apresentadas pelos diferentes setores permitiu delinear um panorama abrangente da realidade brasileira no que se refere à proteção de dados pessoais no contexto das relações de trabalho. Mais do que identificar práticas isoladas, esse conjunto de insumos evidencia a existência de elementos estruturantes que, de forma transversal, moldam a forma como os direitos à privacidade e à proteção de dados se concretizam — ou encontram limitações — no cotidiano das pessoas trabalhadoras.

Nesse sentido, a presente seção tem como objetivo contextualizar os principais fatores sistêmicos que caracterizam essa realidade, servindo como base interpretativa para os temas desenvolvidos ao longo do relatório. Trata-se de compreender o ambiente laboral como um espaço complexo, marcado por diferentes arranjos jurídicos, relações assimétricas e crescente incorporação de tecnologias baseadas em dados, que impactam diretamente a forma como informações pessoais são geradas, apropriadas, tratadas e compartilhadas.

### 4.1 Atores no tratamento de dados no contexto laboral

A partir das categorias estabelecidas pela Lei Geral de Proteção de Dados (LGPD), é possível identificar os principais atores envolvidos no tratamento de dados pessoais no contexto laboral — titulares, controladores e operadores — reconhecendo que essas figuras assumem configurações específicas nas relações de trabalho.

Os titulares correspondem, essencialmente, às pessoas trabalhadoras, mas essa categoria não é homogênea. Ela abrange diferentes formas de inserção no mundo do trabalho, cada uma com níveis distintos de proteção e exposição a riscos.

Destacam-se, nesse contexto:

- **Servidores públicos:** regidos por estatutos próprios (regime jurídico único), com direitos e deveres específicos. O controle de seus dados ocorre no âmbito da administração pública, submetidos a regimes de transparência e sigilo próprios, e à tensão entre a publicidade de dados (exigida pela Lei de Acesso à Informação) e a privacidade;
- **Empregados regidos pela CLT:** possuem vínculo formal de emprego regido pela CLT, com maior arcabouço protetivo (estabilidade relativa, direitos coletivos). O tratamento de seus dados é em grande parte justificado por obrigação legal e execução do contrato, mas enfrenta desafios como coleta excessiva (biometria, geolocalização, monitoramento de produtividade), consentimento frágil e decisões automatizadas, especialmente em recursos humanos;
- **Trabalhadores no regime PJ:** embora formalmente constituídos como pessoas jurídicas, esses trabalhadores frequentemente prestam serviços sob condições que envolvem pessoalidade, subordinação e habitualidade. Apesar disso, não se beneficiam das proteções típicas da legislação trabalhista. Ainda assim, seus dados pessoais são tratados pelo contratante, o que gera desafios relevantes, como a ausência de representação coletiva

estruturada, a prevalência de contratos de adesão e o tratamento — inclusive de dados sensíveis — sem salvaguardas adequadas;

- **Trabalhadores autônomos sem contrato formal:** correspondem àqueles que prestam serviços de forma eventual ou sem vínculo jurídico estruturado, muitas vezes por meio de mediação digital, embora não exclusivamente. Ainda que não se configure relação de emprego, há tratamento de dados pessoais dessas pessoas no contexto da prestação de serviços, o que demanda a observância dos princípios e obrigações previstos na legislação de proteção de dados;
- **Trabalhadores plataformizados:** correspondem àqueles cuja atividade é intermediada e organizada por plataformas digitais, nas quais a gestão do trabalho ocorre por meio de sistemas automatizados e algoritmos em tempo real. Nesse modelo, a execução, a distribuição de tarefas e a avaliação de desempenho são fortemente orientadas pela lógica da datificação e pela infraestrutura tecnológica. Diferentemente das relações tradicionais de emprego, esse arranjo não se estrutura predominantemente a partir do poder diretivo humano direto, mas de mecanismos de controle algorítmico, que passam a exercer papel central na organização e regulação da atividade laboral.

Essa diversidade evidencia que os desafios de proteção de dados variam significativamente conforme o tipo de vínculo, sendo mais intensos em contextos de menor proteção.

Os controladores, por sua vez, são as pessoas jurídicas que se beneficiam do trabalho de alguém, seja com relação jurídica trabalhista, cível ou qualquer outra forma de contratação da força de trabalho, definindo as finalidades e os meios de tratamento dos dados. No contexto laboral, incluem:

- **Governos:** administração pública direta e indireta (municipal, estadual, federal) que tratam dados de servidores, empregados públicos, terceirizados e prestadores. Sujeitos à LGPD (arts. 23 e 24) e à Lei de Acesso à Informação, vivem a tensão entre publicidade e privacidade;
- **Empresas:** pessoas jurídicas de direito privado que contratam trabalhadores sob regime CLT, PJ ou autônomo;
- **Plataformas:** empresas que tem como interface e mediação com as pessoas trabalhadoras meios digitais que intermedeiam serviços, controlam e organizam o trabalho por meio de algoritmos, exercendo controle efetivo sobre a execução do serviço.

Já os operadores, em geral são as pessoas jurídicas, que realizam o tratamento em nome dos controladores, desempenhando funções técnicas e operacionais, contratadas com a responsabilidade de processar os dados a partir do que o controlador está legalmente autorizado a realizar, sendo simplesmente um atravessador por questões técnicas:

- **Terceirizados de atividade meio:** empresas contratadas para atividades como folha de pagamento (payroll), recrutamento e seleção (R&S), benefícios (vale-refeição, plano de saúde), treinamentos corporativos, etc. Eles têm acesso a dados pessoais e sensíveis dos

trabalhadores, mas devem atuar apenas sob instrução legítima do controlador (contrato de operação – art. 39 da LGPD)

- **Provedores de serviços digitais e armazenamento (nuvem):** provedores de serviços digitais e armazenamento em nuvem, que armazenam e processam dados de trabalhadores em infraestrutura frequentemente localizada no exterior;
- **Provedores de sistemas:** fornecem softwares de gestão empresarial (ERP), sistemas de RH, plataformas de monitoramento de produtividade, ferramentas de avaliação de desempenho, dentre outros.

## 4.2 Assimetria estrutural das relações de trabalho

Um dos elementos centrais identificados é a natureza estruturalmente assimétrica da relação de trabalho. O trabalhador, reconhecido como parte hipossuficiente, encontra-se em posição de vulnerabilidade diante do empregador ou contratante, que detém poder sobre aspectos essenciais como renda, permanência no vínculo e organização da atividade.

Essa assimetria impacta diretamente a proteção de dados, especialmente no que se refere à validade do consentimento e à possibilidade real de contestação de práticas de tratamento. Em muitos casos, a dependência econômica limita a liberdade de escolha, o que exige cautela na utilização do consentimento como hipótese legal e reforça a necessidade de outras salvaguardas, buscando limitar a exploração desmedida de informações pessoais.

Nesse contexto, o exercício do poder diretivo (art. 2º da CLT) — que confere ao empregador prerrogativas de direção, fiscalização e disciplina da atividade laboral — não é absoluto, e deve ser interpretado à luz dos direitos fundamentais, especialmente o direito à privacidade previsto na Constituição Federal. Deve ser exercido em harmonia com a dignidade e a valorização do trabalho, com proporcionalidade, restrição a local e horário de trabalho, finalidades lícitas e específicas, vedando-se práticas invasivas ou de interesse meramente exploratório. Isso implica reconhecer que o tratamento de dados deve observar limites claros, relacionados à finalidade, à proporcionalidade e à proteção da dignidade da pessoa trabalhadora.

A privacidade, por sua vez, não se extingue com o ingresso no ambiente de trabalho. Trata-se de direito fundamental, previsto no art. 5º, X, CF, com proteção reforçada nesse contexto, abrangendo a autodeterminação informativa e a garantia de que o trabalhador não seja reduzido a processos automatizados ou métricas opacas que comprometam sua dignidade. O tratamento de dados só é legítimo quando respeita a expectativa razoável de privacidade e garante proteção adicional no ambiente digital, como o direito à desconexão e o controle sobre sistemas biométricos ou de geolocalização desproporcionais.

## 4.3. Ciclo de vida dos dados no Contexto Laboral

O tratamento de dados pessoais no ambiente de trabalho ocorre de forma contínua ao longo de todo o ciclo da relação laboral, abrangendo fases distintas, mas interdependentes.

A **fase pré-contratual** abrange todas as operações de tratamento de dados pessoais realizadas desde a prospecção de candidatos até a decisão de contratar ou não o trabalhador. Inclui, entre outras atividades: recebimento e análise de currículos, realização de entrevistas, aplicação de testes de conhecimento ou psicológicos, verificações de antecedentes (criminais, profissionais ou patrimoniais), consulta a redes sociais ou bases de terceiros, e uso de ferramentas automatizadas de triagem e avaliação de candidatos

A **fase contratual** corresponde ao período compreendido entre o início e o término da prestação de serviços (vínculo empregatício, autônomo, temporário, plataformizado). Envolve o tratamento contínuo de dados pessoais para para viabilizar a execução do trabalho, incluindo: execução das obrigações contratuais (pagamento de salários, controle de jornada, concessão de benefícios); cumprimento de obrigações legais e regulatórias (retenções fiscais, previdenciárias, comunicações a órgãos públicos, registros de saúde ocupacional); exercício do poder diretivo do empregador ou contratante (avaliações de desempenho, alocação de tarefas, aplicação de sanções disciplinares); monitoramento da atividade laboral (geolocalização, biometria, captura de tela, registro de teclas, análise de produtividade); e, muitas vezes, uso secundário de dados.

Já a **fase pós-contratual** é o período subsequente ao término da relação de trabalho, independentemente da causa (pedido de demissão, dispensa, conclusão do contrato, falecimento). Os dados pessoais do trabalhador permanecem sob a guarda do antigo empregador ou contratante por determinados prazos. Após o fim do prazo de guarda, os dados são eliminados ou anonimizados. O trabalhador mantém, nessa fase, direitos como acesso, retificação e, quando cabível, eliminação dos dados.

Essa abordagem evidencia que a proteção de dados não se limita ao momento da execução do trabalho, mas acompanha toda a trajetória da pessoa trabalhadora.

#### 4.4. Economia Digital, datificação e plataformização

A proteção de dados no contexto laboral deve ser compreendida à luz das transformações da economia contemporânea, que é estruturada a partir de uma nova cadeia produtiva digital e de dados, liderada por grandes empresas transnacionais que controlam a infraestrutura tecnológica, incluindo serviços de nuvem, software e plataformas. Essa cadeia produtiva posiciona-se como base das demais cadeias setoriais (agronegócio, indústria, serviços), que se tornam dependentes dessa infraestrutura estrangeira.

Nesse cenário, destaca-se o fenômeno da **datificação**, que consiste na conversão de atividades humanas em dados passíveis de análise, automação e uso em sistemas de inteligência artificial. Esse processo ocorre de forma contínua e, muitas vezes, invisível ao titular, que cede seus dados, através do aceite do "Termos de Uso", como condição para utilizar ferramentas digitais.

A **plataformização** refere-se à reorganização da produção e do trabalho em torno de plataformas digitais que funcionam como intermediárias entre oferta e demanda de serviços,

bens e trabalho. No âmbito laboral, esse fenômeno abrange desde trabalhadores de aplicativos de transporte e entrega até profissionais de saúde, educação e outras áreas que operam por meio de plataformas. Nessas configurações, a gestão do trabalho é mediada por algoritmos que controlam o direcionamento de demandas, a alocação de tarefas, a definição de preços, a avaliação de desempenho e, em muitos casos, a suspensão ou bloqueio do acesso à plataforma.

#### **4.5 Infraestrutura digital e dependência tecnológica**

Os serviços digitais e de armazenamento em nuvem constituem a base da economia de dados, permitindo o processamento em larga escala de informações sem necessidade de infraestrutura própria. Trata-se de sistemas remotos que oferecem capacidade computacional, servidores, bancos de dados, redes e softwares sob demanda, tipicamente operados por grandes provedores transnacionais. Esses serviços permitem que controladores de dados armazenem enormes volumes de informações pessoais e operacionais sem necessidade de infraestrutura própria, mediante contratos de adesão e termos de uso padronizados. No entanto, essa dependência de provedores, muitas vezes transnacionais, introduz desafios adicionais relacionados à governança, segurança e soberania dos dados.

#### **4.6 Estrutura analítica do relatório**

A partir dessa contextualização, o relatório se organiza em quatro eixos temáticos interdependentes, que permitem aprofundar os principais desafios da proteção de dados no contexto laboral.

De forma estruturada, o trabalho se debruça sobre:

- **Eixo 1 – Princípios e hipóteses legais**
- **Eixo 2 – Transparência e exercício de direitos dos titulares**
- **Eixo 3 – Monitoramento e produtividade**
- **Eixo 4 – Diálogo social e negociação coletiva**
- 

Esses eixos não se apresentam de forma isolada, mas se articulam de maneira integrada, refletindo a complexidade do tema e a necessidade de uma abordagem sistêmica. A partir deles, busca-se não apenas identificar riscos e desafios, mas também apontar caminhos para o aprimoramento da proteção de dados no contexto laboral brasileiro.

Nesse contexto, o primeiro eixo assume papel estruturante, ao estabelecer as bases jurídicas e principiológicas que orientam todo o tratamento de dados nas relações de trabalho.

## 5. Princípios e Hipóteses Legais no Tratamento de Dados Pessoais no Contexto Laboral

Neste primeiro eixo, o relatório expõe as principais abordagens apresentadas pelos especialistas e instituições convidadas acerca da aplicação dos princípios e das hipóteses legais da Lei Geral de Proteção de Dados Pessoais (LGPD) no tratamento de dados pessoais no contexto das relações de trabalho.

As abordagens partem de experiências acadêmicas, práticas e institucionais diversas, com o propósito de construir uma visão mais abrangente e plural, conferindo maior amplitude técnica aos subsídios e, por conseguinte, ao relatório.

As reflexões convergem, em boa medida, na afirmação de que a aplicação da LGPD nesse campo exige um rigor interpretativo qualificado, em razão da assimetria estrutural que caracteriza tais relações, dos diferentes níveis de subordinação e dependência econômica e da natureza dinâmica do vínculo laboral, que se desenvolve em fases distintas — pré-contratual, contratual e pós-contratual.

Nesse contexto, afasta-se a compreensão de que a simples identificação de uma hipótese legal seja suficiente para legitimar o tratamento de dados pessoais, consolidando-se o entendimento de que os princípios previstos no artigo 6º da LGPD exercem função estruturante, antecedendo e condicionando a própria escolha da base jurídica aplicável.

Ana Rita Biba Gomes de Almeida defende que a análise jurídica do tratamento de dados no ambiente laboral deve iniciar-se pelos princípios da finalidade, da necessidade e da transparência, que funcionam como critérios prévios de validação da legitimidade do tratamento.

Para a especialista, a base legal não constitui autorização autônoma, mas elemento dependente de uma verificação prévia de compatibilidade do tratamento com a finalidade declarada, de proporcionalidade em relação aos riscos envolvidos e de respeito aos direitos do titular.

Tal racionalidade é expressa em um modelo analítico em “funil”, no qual os princípios delimitam o espaço de atuação da base legal, que deve ser acompanhada de garantias efetivas ao titular e de mecanismos de governança.

A especialista ainda ressalta que, embora a LGPD não distinga formalmente vínculos empregatícios e não empregatícios, o grau real de subordinação, dependência econômica e poder de direção deve influenciar a intensidade de incidência dos princípios, especialmente quanto à avaliação da finalidade, da proporcionalidade e da expectativa legítima do titular.

Vólia Bomfim, por sua vez, atribui aos princípios uma dimensão material mais incisiva, sustentando que boa-fé, finalidade e necessidade operam como limites reais ao exercício do poder empregatício e do poder organizacional. A autora observa que, nas relações com vínculo empregatício, a presunção de subordinação impõe maior rigor no controle do tratamento de dados, enquanto, nas relações sem vínculo formal, a autonomia aparente não autoriza práticas

invasivas de coleta ou vigilância quando subsiste dependência econômica, técnica ou informacional. A boa-fé, nesse cenário, exige previsibilidade, coerência e lealdade no uso dos dados ao longo de toda a relação.

Em complemento, a especialista estrutura a aplicação das bases legais conforme as fases da relação laboral, reconhecendo espaço limitado para consentimento na fase pré-contratual, predominância da execução do contrato e do cumprimento de obrigação legal na fase contratual e centralidade dessas mesmas bases na fase pós-contratual, sempre sob a perspectiva da dignidade do trabalhador e da proteção de sua privacidade. |

A leitura faseada da relação de trabalho é reiterada por diferentes especialistas como elemento indispensável à correta aplicação da LGPD. Destaca-se que os dados pessoais percorrem um ciclo de vida multifásico e que a legitimidade de um tratamento não se mantém automaticamente ao longo dessas etapas.

Ana Rita Biba Gomes de Almeida enfatiza que dados coletados antes da contratação, durante a execução contratual ou após o seu término submetem-se a contextos jurídicos distintos, sendo inadequada sua reutilização automática entre fases.

Selma Carloto, a partir de uma perspectiva prática, identifica na ausência dessa leitura faseada uma das principais causas de irregularidades, apontando como situações recorrentes a coleta excessiva na fase pré-contratual, o uso indevido do consentimento durante o contrato e a retenção prolongada de dados após o encerramento da relação.

Carolina Tupinambá relaciona diretamente essa estrutura temporal ao dever de transparência, defendendo que ele varia conforme a fase da relação e o tipo de vínculo. Em relações empregatícias, a transparência deve ser intensificada em razão da vulnerabilidade do trabalhador, exigindo maior detalhamento e inteligibilidade.

Nas relações sem vínculo formal, embora haja maior autonomia aparente, a transparência permanece essencial, especialmente em contextos de monitoramento, avaliação e uso intensivo de dados. A autora destaca que, na fase pré-contratual, devem ser claramente informadas as finalidades da coleta; durante a execução contratual, devem ser explicitados algoritmos, métricas e impactos de decisões automatizadas; e, na fase pós-contratual, devem ser definidos e comunicados os critérios de retenção e descarte.

Nesse mesmo sentido, Gaudio Ribeiro sustenta que a análise jurídica deve considerar simultaneamente a dimensão temporal da relação e sua natureza jurídica, advertindo que a distinção entre vínculos não pode ser meramente formal, devendo refletir o grau efetivo de subordinação e controle.

No exame das fases, observa-se que, na etapa pré-contratual, prevalece a orientação pelos princípios da finalidade, necessidade e transparência, vedando-se a coleta genérica ou prospectiva de dados.

O consentimento é admitido apenas excepcionalmente, desde que livre, específico e sem prejuízo em caso de recusa, conforme destacam Selma Carloto e Tatiana Bhering Roxo.

Na fase contratual, predominam a execução do contrato e o cumprimento de obrigação legal, devendo o tratamento respeitar a limitação de finalidade, a boa-fé e a transparência qualificada.

Nesse contexto, Vólia Bomfim ressalta que a previsão contratual não legitima ilimitadamente o tratamento, enquanto Ana Rita alerta para o risco de expansão indevida das finalidades sob justificativas genéricas.

O legítimo interesse é admitido, especialmente em atividades de segurança e monitoramento, mas depende de testes rigorosos de balanceamento, como indicado por Selma Carlotto e Tatiana Bhering Roxo.

Na fase pós-contratual, consolida-se o entendimento de que a retenção deve ser limitada ao necessário, sendo vedada a manutenção indefinida sem finalidade legítima, com destaque para a necessidade de descarte seguro e de transparência quanto aos prazos de retenção.

No plano institucional, a FIESP sustenta que o tratamento de dados pessoais possui caráter estrutural à relação de trabalho, sendo indispensável ao seu funcionamento desde a fase pré-contratual até o pós-contrato, e identifica como bases centrais a execução do contrato, o cumprimento de obrigação legal, o exercício regular de direitos e o legítimo interesse, atribuindo ao consentimento caráter residual.

A Confederação Nacional da Indústria enfatiza que o tratamento decorre da própria estrutura do vínculo empregatício, sendo necessário ao cumprimento de obrigações legais e à organização das atividades, defendendo que a aplicação da LGPD não deve comprometer o poder diretivo nem a livre iniciativa.

A contribuição da FIRJAN agrega a esse conjunto uma dimensão de maior densidade operacional e metodológica, ao enfatizar que as finalidades do tratamento devem ser estritamente vinculadas à gestão do vínculo empregatício e ao cumprimento de obrigações legais, devendo ser legítimas, específicas e previamente informadas ao titular, sendo vedada a utilização para finalidades incompatíveis ou excessivamente genéricas.

A entidade destaca, ainda, que o tratamento deve observar de forma sistemática os princípios da finalidade, da necessidade, da transparência, da proporcionalidade e da responsabilização, atribuindo centralidade à delimitação clara das finalidades e à vedação da retenção genérica de dados. O princípio da necessidade é apresentado como critério de racionalização do tratamento, destinado a evitar excessos sem inviabilizar a atividade empresarial.

Além disso, a FIRJAN confere especial destaque ao princípio da responsabilização e prestação de contas (accountability), defendendo a adoção de instrumentos concretos de governança, como inventários de dados, matrizes de bases legais, registros de atividades de tratamento e relatórios de impacto, integrados a estruturas de compliance e gestão de riscos.

A entidade também chama atenção para riscos decorrentes do uso inadequado das hipóteses legais, como o desvio de finalidade, a coleta excessiva de dados, o uso discriminatório de informações e a falta de transparência, bem como para a inadequação da indicação simultânea de múltiplas hipóteses legais para uma mesma operação, prática que pode comprometer a clareza informacional e a segurança jurídica.

Outras contribuições aprofundam dimensões específicas do tema.

O Instituto ALANA sustenta que o tratamento de dados de crianças e adolescentes deve ser orientado pelo princípio do melhor interesse do titular, exigindo salvaguardas reforçadas e restringindo o uso de determinadas bases legais.

Carlos Fernandes Coninck, assessor jurídico da CUT, critica a utilização do consentimento, apontando que sua validade é comprometida pela assimetria das relações de trabalho, e enfatiza a necessidade de observância dos princípios da não discriminação e da minimização.

O Data Privacy defende uma abordagem baseada em transparência ativa, proporcionalidade e minimização, com especial rigor na utilização do legítimo interesse.

Tatiana Bhering Roxo sistematiza a matéria destacando a centralidade das hipóteses contratuais e legais, a necessidade de critérios rigorosos para o uso do consentimento e do legítimo interesse e a importância dos princípios da finalidade, necessidade e proporcionalidade como parâmetros de legitimidade.

Em síntese, consolida-se um núcleo comum segundo o qual o tratamento de dados pessoais no contexto laboral deve se fundamentar predominantemente na execução do contrato e no cumprimento de obrigação legal, com uso restrito do consentimento e admissão condicionada do legítimo interesse.

Os princípios da finalidade, necessidade, transparência e proporcionalidade assumem função estruturante, orientando e limitando o tratamento, enquanto a análise deve necessariamente considerar o faseamento da relação de trabalho e o grau de subordinação existente.

A contribuição da FIRJAN busca traduzir esses parâmetros em instrumentos concretos de governança e gestão, reforçando a dimensão operacional da LGPD e contribuindo para a construção de soluções que conciliem proteção de direitos fundamentais e viabilidade das atividades econômicas.

## **6. Transparência e Exercício de Direitos dos Titulares**

Dando sequência à análise dos fundamentos jurídicos e principiológicos, e retomando o caráter estruturante do faseamento da relação de trabalho — já evidenciado no eixo anterior —, passa-se ao exame da transparência e do exercício dos direitos dos titulares no contexto laboral.

No contexto laboral, o tratamento de dados pessoais ocorre de forma contínua ao longo de todo o ciclo de vida da relação de trabalho, desde o recrutamento até a fase pós-contratual, sendo marcado por uma assimetria estrutural entre empregador e trabalhador, uso crescente de tecnologias e exposição constante a decisões baseadas em dados. Nesse cenário, a transparência e o exercício efetivo dos direitos dos titulares assumem papel fundamental para assegurar a dignidade do trabalhador, o equilíbrio da relação e a conformidade com a legislação trabalhista, com a Lei Geral de Proteção de Dados e com a proteção dos direitos fundamentais do trabalhador.

A transparência, nesse contexto, não pode ser compreendida como mera formalidade documental. Ela deve ser ativa, contínua, compreensível e verificável, permitindo que o

trabalhador entenda claramente como e o porquê seus dados serão tratados e tenha condições reais de exercer controle sobre esse tratamento. Sua função principal é reduzir a assimetria informacional inerente à relação de trabalho e viabilizar a autodeterminação informativa.

O principal instrumento de concretização da transparência é o **aviso de privacidade**, que deve informar previamente as atividades de tratamento de dados pessoais, por meio de uma comunicação clara, acessível e contínua, reduzindo a assimetria informacional e assegurando uma relação de confiança entre empregador e trabalhador, no contexto do tratamento de dados pessoais.

Para cumprir sua função, o aviso de privacidade deve ser específico para os trabalhadores, usar linguagem simples, acessível e adequada ao contexto laboral, ser atualizado ao longo da relação de trabalho, devendo conter: finalidades específicas e compreensíveis, hipótese legal aplicável, categorias de dados tratados, tecnologias utilizadas — especialmente em contextos de monitoramento e uso de algoritmos — compartilhamentos, prazos de retenção, direitos dos titulares e canais de atendimento, que devem ser acessíveis, rápidos e eficazes.

#### **Estrutura mínima esperada do Aviso de Privacidade:**

- ❖ Identificação do Controlador
- ❖ Finalidades específicas por fase (recrutamento, contrato, pós-contrato)
- ❖ Hipótese legal por finalidade
- ❖ Tipos de dados tratados
- ❖ Compartilhamento com Terceiros
- ❖ Prazo de Retenção
- ❖ Direitos do Titular
- ❖ Canal de Contato
- ❖ Informações sobre monitoramento e tecnologias utilizadas

#### **Boas Práticas de Redação:**

- ❖ Linguagem Simples e Direta
- ❖ Estrutura em perguntas e respostas
- ❖ Atualização constante
- ❖ Comunicação Contínua (não apenas no *onboarding*)

### Importante!

É fundamental ressaltar a distinção entre aviso de privacidade e a hipótese legal do consentimento, sendo o primeiro voltado à informação e o segundo à autorização, esta última de caráter excepcional no contexto laboral, em razão da limitação de liberdade do trabalhador na relação de emprego.

### Cenário Atual

No âmbito da transparência e do exercício dos direitos dos titulares no contexto laboral, a análise dos materiais evidencia que muitas organizações apresentam um grau de conformidade apenas formal, sem efetiva operacionalização das obrigações previstas na Lei Geral de Proteção de Dados.

Os especialistas consultados relataram que, de modo geral, a preocupação não reside na ausência de avisos de privacidade ou de canais de atendimento para o exercício de direitos, mas na qualidade desses instrumentos. Observa-se, com frequência, a existência de documentos genéricos, vagos e pouco informativos, bem como de canais formalmente disponíveis, mas que não são efetivamente utilizados pelos trabalhadores.

Esse cenário dialoga diretamente com a compreensão, já consolidada no eixo anterior, de que o tratamento de dados no contexto laboral é contínuo, multifásico e marcado por assimetria estrutural, o que intensifica a exigência de transparência. Conforme destacado por Ana Rita Bibá Gomes de Almeida, a transparência “não é um atributo abstrato, nem se satisfaz com a mera existência formal de documentos”, devendo ser compreendida como elemento essencial para garantir a autodeterminação informativa e a efetividade dos direitos dos titulares.

Na mesma linha, Tatiana Bhering Roxo aponta que a adoção de instrumentos formais, como avisos de privacidade, não tem sido suficiente para assegurar a efetividade da proteção de dados no ambiente laboral, especialmente quando estruturados de forma genérica ou padronizada.

Um exemplo recorrente diz respeito à utilização de **avisos de privacidade genéricos**, como “fins administrativos e operacionais”, incapazes de traduzir as reais finalidades do tratamento de dados pessoais dos trabalhadores. Nesses casos, a ausência de especificidade impede a compreensão do tratamento e, conseqüentemente, dificulta o exercício dos direitos pelos titulares.

A correção desse tipo de prática exige a redefinição do aviso de privacidade com base em finalidades concretas e diretamente vinculadas ao contexto laboral, tais como formalização do vínculo, gestão de folha de pagamento, controle de jornada e cumprimento de obrigações legais, além da explicitação clara das etapas do tratamento.

Outro ponto crítico identificado refere-se à ausência de transparência em relação ao uso de tecnologias de monitoramento. Situações em que sistemas de análise de produtividade ou registro de atividades são utilizados sem adequada comunicação aos trabalhadores evidenciam não apenas falhas informacionais, mas também limitações concretas ao exercício de direitos, como o direito de oposição. A conformidade, nesses casos, pressupõe detalhamento das ferramentas utilizadas, dos dados coletados e dos impactos dessas práticas, especialmente quando associadas a decisões de gestão.

Essa preocupação também é reforçada no material de Gáudio Ribeiro de Paula, ao destacar que a transparência deve abranger não apenas a existência do tratamento, mas também as tecnologias utilizadas, os critérios envolvidos e a efetividade dos canais de resposta, sob pena de se configurar um cenário de “compliance meramente formal”.

Nesses casos, a conformidade exige o detalhamento das ferramentas utilizadas, dos dados coletados e dos impactos dessas práticas, especialmente quando associadas a decisões de gestão.

Adicionalmente, a **fragilidade dos canais de atendimento** para o exercício de direitos emerge como um dos principais entraves à efetividade da LGPD no contexto laboral. Embora tais canais frequentemente existam, sua utilização é limitada, seja pela falta de conhecimento dos trabalhadores sobre sua existência, seja pela ausência de confiança, muitas vezes associada ao receio de exposição ou de possíveis represálias.

A existência de canais formais sem estrutura operacional adequada — sem definição de prazos, responsáveis ou mecanismos de acompanhamento — configura um cenário de transparência meramente aparente. A superação dessas limitações demanda a criação de canais efetivos, acessíveis e confiáveis, com fluxos claramente definidos, integração com o Encarregado pelo tratamento de dados e mecanismos que permitam o registro, a auditoria e a revisão das solicitações apresentadas pelos titulares.

## Boas Práticas para canais de atendimento:

Os canais devem ser:

- ❖ acessíveis
- ❖ conhecidos pelos trabalhadores
- ❖ independentes e confiáveis
- ❖ eficientes e tempestivos
- ❖ livres de retaliação
- ❖ auditáveis

### Convergências e Tensões

A análise conjunta dos materiais revela convergência quanto à estrutura básica da proteção de dados no ambiente laboral. Em primeiro lugar, há consenso quanto à existência de uma assimetria de poder e de informação entre empregador e trabalhador, elemento que, como já destacado, intensifica a necessidade de transparência qualificada.

Também se observa alinhamento quanto à centralidade da transparência como mecanismo de redução dessa assimetria, devendo ser ativa, compreensível e contínua. Nesse sentido, conforme destacado por Ana Rita Bibá Gomes de Almeida, a transparência, no contexto laboral, não se esgota na existência formal de documentos, devendo garantir ao trabalhador informações claras, precisas e acessíveis sobre o tratamento de seus dados, especialmente em ambientes marcados por tratamentos contínuos e tecnicamente opacos.

Ainda nesse eixo de convergência, há consenso quanto à necessidade de limites ao monitoramento e ao uso de tecnologias, especialmente no que se refere à proporcionalidade, à não discriminação e à limitação de finalidade, sendo fundamental que tais práticas sejam devidamente informadas ao trabalhador. Essa exigência se intensifica na medida em que o monitoramento se torna mais intrusivo, exigindo maior grau de transparência e justificativa.

Por fim, destaca-se convergência quanto aos riscos associados à automação e ao uso de inteligência artificial, com reconhecimento da necessidade de mecanismos efetivos de controle, explicabilidade e direito à revisão de decisões automatizadas. Como também apontado nas contribuições analisadas, a transparência, nesses casos, deve abranger não apenas a existência da decisão automatizada, mas também os critérios gerais envolvidos e seus impactos sobre o trabalhador.

Apesar das convergências, os materiais também evidenciam divergências relevantes. Uma das principais diz respeito ao nível de transparência exigido, especialmente em relação a sistemas

algorítmicos. Há divergência entre modelos que defendem transparência ampliada – com maior abertura sobre critérios e funcionamento de sistemas - e aqueles que reconhecem limites decorrentes de complexidade técnica ou da necessidade de proteção de segredos comerciais.

Além disso, observam-se diferenças quanto ao grau de rigor regulatório. Enquanto algumas abordagens defendem maior intervenção normativa, com definição mais detalhada de parâmetros pela autoridade reguladora, outras privilegiam soluções baseadas em governança interna, boas práticas e autorregulação. Essa tensão reflete, em última análise, o desafio de equilibrar segurança jurídica, proteção de direitos e viabilidade operacional no contexto do tratamento de dados no ambiente de trabalho.

### **Boas práticas identificadas**

Dentre as boas práticas consolidadas, destaca-se a elaboração de avisos de privacidade específicos para trabalhadores, com linguagem acessível e atualização contínua, integrados aos processos de *onboarding* e às rotinas de comunicação interna. Essa prática responde diretamente ao diagnóstico anteriormente identificado, no qual a transparência, quando tratada de forma genérica ou meramente formal, compromete a compreensão do tratamento e o exercício de direitos.

Nesse sentido, conforme destacado por Ana Rita Bibá Gomes de Almeida, a transparência no contexto laboral deve assegurar a disponibilização de informações claras, precisas e facilmente acessíveis, especialmente em cenários de tratamento contínuo e multifásico de dados, nos quais o trabalhador está exposto a processos muitas vezes tecnicamente opacos.

A transparência deve ser complementada por canais efetivos de exercício de direitos, com prazos definidos, múltiplos meios de acesso e garantia de ausência de retaliação, de modo a assegurar não apenas a existência formal desses mecanismos, mas sua efetiva utilização pelos trabalhadores.

No plano organizacional, recomenda-se a capacitação contínua das áreas envolvidas, especialmente recursos humanos, bem como a disseminação de boas práticas entre todos os trabalhadores, contribuindo para a construção de uma cultura organizacional orientada à proteção de dados.

Dessa forma, a transparência e o exercício de direitos no contexto laboral devem ser tratados como eixo estruturante da governança organizacional, constituindo elemento essencial para a redução das assimetrias informacionais e para a proteção da dignidade da pessoa trabalhadora.

## **7. Tecnologias de monitoramento e produtividade**

O ambiente laboral contemporâneo conta cada vez mais com ferramentas que seguem os padrões da indústria de datificação e plataformação das atividades de trabalho. Essas ferramentas exercem funções de controle, vigilância e análise de produtividade, incluindo captura de tela, registro de teclas, geolocalização, biometria, câmeras de vídeo, sensores de

movimento, entre outras tantas possibilidades de geração de dados. Os dados gerados alimentam sistemas de desempenho e análises de organização do trabalho, sendo também frequentemente reaproveitados pelas próprias empresas fornecedoras para seus próprios interesses, caracterizando, de forma sistêmica, um uso secundário inadequado. A seguir, são apresentadas as principais questões identificadas nas discussões do GT1 em torno dos parâmetros do Eixo 3.

## **7.1 Proporcionalidade e limitação à finalidade**

A utilização de ferramentas de controle e vigilância no ambiente laboral encontra fundamento no poder diretivo do empregador (art. 2º da CLT), mas esse poder não é absoluto. Para que seja legítimo, o monitoramento deve observar rigorosamente os princípios da finalidade específica, da necessidade e da proporcionalidade (art. 6º da LGPD). Isso significa que a coleta, geração e apropriação de dados deve estar estritamente vinculada a uma finalidade concreta, lícita e previamente informada ao trabalhador (titular de dados), sendo vedada a utilização de finalidades amplas ou genéricas (como "melhoria de processos" ou "segurança") que costumeiramente são utilizadas como justificativa para vigilância sistemática ou para usos secundários não comunicados.

Na prática, observa-se que sistemas de monitoramento de produtividade frequentemente capturam informações que vão além do estritamente necessário, como capturas de tela durante intervalos, geolocalização fora do horário de serviço, acesso a câmeras em locais de descanso, transformando essa gama de informações em dados comportamentais. A jurisprudência trabalhista e as diretrizes internacionais apontam que a legitimidade do monitoramento depende da demonstração de que: (i) há uma finalidade específica e legítima (ex.: saúde e segurança do trabalho); (ii) não existem meios menos invasivos para alcançar a mesma finalidade; (iii) a geração é limitada ao necessário e temporariamente restrita. Além disso, o monitoramento deve ser limitado ao local e horário de trabalho, vedando-se a geração e apropriação de dados fora da jornada ou em dispositivos pessoais do trabalhador (salvo situações excepcionais e devidamente justificadas). Qualquer geração de dados sobre o trabalhador sem comunicação prévia é amplamente rejeitada por ser prática invasiva, desproporcional e abusiva.

Diante desse cenário, a observância rigorosa dos princípios da finalidade, da necessidade e da proporcionalidade não se configura apenas como exigência legal, mas como condição essencial para a legitimidade do monitoramento no ambiente de trabalho. A ausência desses parâmetros compromete a proteção de dados pessoais dos trabalhadores e amplia riscos de práticas abusivas, exigindo das organizações a adoção de medidas claras de limitação, transparência e controle sobre o tratamento de dados.

## **7.2 Parâmetros éticos e técnicos para biometria, geolocalização, câmeras e softwares de produtividade**

O uso dessas tecnologias exige um equilíbrio entre as necessidades organizacionais e os direitos fundamentais dos trabalhadores. A partir das contribuições dos especialistas e da ANPD, destacam-se os seguintes parâmetros:

- **Biometria (reconhecimento facial, impressão digital, íris, voz):** por envolver o tratamento de dados pessoais sensíveis, nos termos do art. 5º, II, da LGPD, e considerando sua natureza intrínseca e imutável — que impede substituição em caso de violação —, seu uso deve ser excepcional e restrito a situações em que haja risco relevante e devidamente justificado, como em contextos de alta criticidade ou prevenção de fraudes graves. Nesses casos, é indispensável a realização de avaliação concreta de necessidade e proporcionalidade, bem como a oferta de alternativas menos invasivas, como uso de crachá ou PIN, para os trabalhadores que não possam ou não desejem utilizar tais tecnologias, no caso de a hipótese autorizativa ser o consentimento ou ainda nos casos em que é possível atingir a finalidade de forma menos intrusiva ao titular de dados.

Ademais, a Resolução ANPD nº 23/2025 estabelece requisitos específicos de transparência e salvaguardas para esse tipo de tratamento, reconhecendo a geração de dados biométricos de trabalhadores como atividade de alto risco, a qual deve ser precedida da elaboração de Relatório de Impacto à Proteção de Dados (RIPD). As contribuições analisadas indicam, ainda, que, na maioria dos casos, o uso de biometria pode ser substituído por outros mecanismos de autenticação menos intrusivos e igualmente eficazes.

- **Geolocalização:** Quando utilizada para controle de jornada, rastreamento de veículos ou verificação de presença em campo, deve ser ativada apenas durante a jornada de trabalho e com desligamento automático fora do expediente. A preferência é pelo registro por evento (check-in/check-out, confirmação de chegada/saída) ou por amostragem, não por rastreamento contínuo. A geração não pode ser utilizada para controle comportamental, fiscalização de condutas ou avaliação de produtividade, sob pena de desvio de finalidade. A geolocalização fora do expediente ou para inferir atividades pessoais (ex.: frequência a locais de lazer, consultas médicas, participação em manifestações) viola a privacidade. O TST já validou a geolocalização como prova de jornada, desde que limitada ao local e horário de trabalho (ROT-23218-21.2023.5.04.0000). Para todos os casos, é necessário avaliar se a geolocalização é realmente a única forma de alcançar a finalidade operacional.
- **Câmeras de segurança (CFTV):** a utilização de sistemas de videomonitoramento deve estar vinculada a finalidades legítimas e previamente definidas, especialmente relacionadas à proteção patrimonial e à segurança de pessoas. Para garantir a proporcionalidade do tratamento, a captação de imagens deve se restringir a áreas comuns e de circulação, com sinalização visível e existência de política interna clara e acessível aos trabalhadores. A instalação desses sistemas em espaços de natureza privada — como áreas de descanso, vestiários, refeitórios ou sanitários — é vedada, em razão do elevado risco à privacidade. Da mesma forma, a gravação contínua de postos de trabalho demanda justificativa robusta e transparência quanto às suas finalidades e limites. No que se refere à gestão das informações coletadas, a retenção das imagens deve

observar critérios de necessidade e temporalidade, não sendo admissível sua manutenção por prazo indeterminado. O acesso às imagens deve ser restrito a pessoas autorizadas e sujeito a mecanismos de controle e auditoria. Ademais, a utilização das gravações para fins disciplinares ou de avaliação de desempenho deve ser afastada, sob pena de desvio de finalidade. Por fim, destaca-se que a efetividade dessas salvaguardas está diretamente relacionada à garantia de ciência e compreensão por parte dos trabalhadores, elemento indissociável da proteção de seus direitos no ambiente laboral.

- **Softwares de monitoramento de produtividade ("boss ware"):** Ferramentas que capturam cliques, tempo de inatividade, janelas ativas, uso de aplicativos, webcam, áudio ambiente e reconhecimento facial - inclusive para análise de emoções - são consideradas altamente intrusivas. Especialistas apontam que tais práticas geram impactos negativos relevantes, como aumento de estresse, ansiedade, comprometendo a saúde mental dos trabalhadores, além de produzirem dados excessivos, muitas vezes sem base legal adequada ou justificativa clara. No plano jurídico, a jurisprudência do Tribunal Superior do Trabalho - TST tem validado o uso dessas ferramentas apenas quando há ciência prévia inequívoca do trabalhador e desde que o monitoramento não ultrapasse os limites necessários e proporcionais à finalidade pretendida. Nesse contexto, o desenho dessas soluções deve ser orientado pelo princípio do "*privacy by default*", privilegiando o menor nível de coleta possível para atingir a finalidade declarada, privilegiando métricas baseadas em entregas e resultados, em detrimento da vigilância contínua do comportamento. Adicionalmente, os fornecedores desse tipo de software fazem parte de um pequeno grupo de grandes empresas estrangeiras de tecnologia, limitando as possibilidades de as organizações brasileiras renunciar a essas empresas na sua operação. Esse tipo de dependência com plataformas de monopólios estrangeiros pode gerar riscos adicionais, especialmente os relacionados com uma utilização secundária dos dados dos trabalhadores pelos próprios fornecedores de softwares de produtividades e/ou organização do trabalho, seja para aprimoramento de serviços, seja para outras finalidades não plenamente transparentes, o que reforça a necessidade de mecanismos robustos de governança e controle sobre esses fluxos de dados.

Nesse contexto, o uso dessas tecnologias deve ser orientado por uma abordagem baseada em risco, com ênfase na minimização de dados, na adoção de alternativas menos intrusivas e na implementação de salvaguardas técnicas e organizacionais adequadas. A conformidade com a LGPD exige não apenas a justificativa do tratamento, mas a demonstração contínua de sua necessidade, proporcionalidade e adequação no ambiente laboral.

### 7.3 Transparência sobre algoritmos de pontuação e ranqueamento

Sistemas automatizados que atribuem notas, níveis ou classificações ao desempenho dos trabalhadores, cujos resultados influenciam promoções, alocação de tarefas, bônus, treinamentos ou até desligamentos, são, em regra, opacos aos próprios trabalhadores. A transparência

algorítmica é uma exigência direta do art. 20 da LGPD, que assegura ao titular o direito à revisão de decisões automatizadas. Essa realidade perpassa trabalhadores de diferentes relações jurídicas, os celetistas, os pejetizados e os plataformizados, em diferentes momentos da sua jornada de contratação, mas sobretudo na fase pré-contratual - quando a empresa precisa atribuir características a um candidato e aferir sobre ele - e na contratual - quando a atividade de trabalho já está ocorrendo, e se vale desses dados da atividade laboral para tomar decisões orientadas por algoritmos.

Nesse cenário, é fundamental reconhecer que o trabalhador, na condição de titular de dados, possui o direito de acessar informações sobre os tratamentos realizados, enquanto o controlador tem o dever de garantir transparência quanto aos dados utilizados e às finalidades envolvidas. A ausência de acesso a essas informações compromete significativamente a capacidade de compreensão e de contestação por parte do trabalhador, enfraquecendo sua posição na relação laboral. Sem visibilidade sobre os dados que são gerados a partir de sua própria experiência e utilizados na tomada de decisões, o trabalhador se vê privado de condições mínimas para dialogar, questionar ou negociar de forma equilibrada.

As entrevistas realizadas pelo GT1 revelaram que grande parte desses algoritmos é mantida sob sigilo empresarial, com trabalhadores desconhecendo quais métricas são utilizadas, como são ponderadas, qual o período de avaliação e como contestar uma pontuação desfavorável. A ausência de transparência impede o exercício do direito de petição e revisão previsto em lei.

Para que o direito seja efetivo, o trabalhador deve ser informado, de forma prévia, clara e acessível, sobre: (i) quais dados são coletados e como alimentam o algoritmo; (ii) os critérios gerais e as métricas utilizadas; (iii) a forma como a pontuação é calculada e interpretada; (iv) quais decisões podem ser afetadas; (v) a possibilidade de revisão humana e os canais de contestação. Não se exige a divulgação de segredos comerciais ou código-fonte, mas sim uma explicação significativa que permita ao trabalhador compreender a lógica da decisão e, se for o caso, questioná-la. A experiência internacional (GDPR, diretrizes da CNIL, ICO) recomenda esse mesmo padrão.

Boas práticas incipientes incluem: disponibilização de dashboards individuais com as métricas utilizadas, possibilidade de solicitar revisão humana da pontuação, e canais de reclamação acessíveis. Além disso, é imprescindível que as empresas mantenham governança algorítmica: inventário de modelos, documentação de testes de viés, procedimentos de revisão humana e registro das decisões automatizadas que impactam os trabalhadores.

A efetividade do direito à revisão de decisões automatizadas depende, portanto, da garantia de transparência significativa e do acesso a informações que permitam ao trabalhador compreender e contestar os critérios utilizados. Sem esses elementos, a utilização de sistemas algorítmicos compromete a autodeterminação informativa e enfraquece a proteção de dados pessoais no contexto das relações de trabalho.

## 7.4 Riscos discriminatórios diretos e indiretos

O uso de ferramentas de monitoramento e análise de produtividade pode gerar ou amplificar discriminações por raça, gênero, idade, condição de saúde, regionalidades, crenças, deficiência ou outras características. A discriminação algorítmica ocorre quando sistemas automatizados produzem resultados adversos desproporcionais sobre determinados grupos, ainda que os critérios sejam aparentemente neutros.

Foram identificados os seguintes mecanismos:

- **Vieses nos dados históricos:** Algoritmos treinados com dados de desempenho passado reproduzem padrões discriminatórios existentes (ex.: avaliações inferiores para mulheres em licença-maternidade, menor pontuação para trabalhadores negros em contextos de racismo estrutural);
- **Métricas enviesadas:** Indicadores como "tempo de inatividade", "número de pausas", "velocidade de digitação" penalizam desproporcionalmente pessoas com deficiências, condições de saúde crônicas, neurodivergências ou aquelas que realizam tarefas de maior complexidade;
- **Penalizações indiretas:** Sistemas que ranqueiam automaticamente os trabalhadores podem direcionar menos tarefas ou tarefas de menor valor para perfis repetidamente mal avaliados, reduzindo sua renda ou oportunidades;
- **Falta de auditoria algorítmica:** A maioria dos empregadores não realiza auditorias periódicas para identificar vieses discriminatórios, e a ausência de RIPD agrava o risco.

Exemplos concretos identificados nas contribuições: softwares que medem tempo de atividade na tela penalizam trabalhadores com responsabilidades familiares; geolocalização usada para avaliar desempenho prejudica quem reside em áreas periféricas; algoritmos de recrutamento treinados com dados históricos podem excluir automaticamente mulheres, negros ou pessoas mais velhas; sistemas de reconhecimento facial podem ter menor precisão para determinados grupos demográficos, gerando bloqueios ou avaliações injustas (caso do iFood citado por Renan Kalil).

Para mitigar esses riscos, as organizações devem realizar testes de viés antes da implantação, adotar RIPD para sistemas de alto risco e garantir a revisão humana significativa antes de qualquer decisão relevante baseada em pontuação automatizada. A auditoria periódica dos resultados é essencial para corrigir desvios e prevenir discriminação. A jurisprudência recente - condenação de plataforma de recrutamento por dano moral coletivo no TRT da 15ª Região - tem reconhecido que o uso de algoritmos com viés discriminatório viola a LGPD, a Constituição e a legislação trabalhista.

A mitigação desses riscos exige a adoção de mecanismos estruturados de governança algorítmica, incluindo testes de viés, auditorias periódicas e revisão humana significativa. A ausência dessas medidas não apenas compromete a conformidade com a LGPD, mas também potencializa a reprodução de desigualdades no ambiente de trabalho, reforçando a necessidade de atuação regulatória e institucional coordenada.

## 7.5 Questões específicas dos trabalhadores plataformizados

Os trabalhadores vinculados a plataformas digitais - como aplicativos de transporte, entrega, serviços domésticos, saúde, educação, dentre outros serviços - enfrentam desafios amplificados em relação aos trabalhadores celetistas. Isso ocorre porque a gestão do trabalho, nesses modelos, é predominantemente mediada por algorítmicos, caracterizando uma forma de controle contínua, abrangente e opaca. Diferentemente das relações tradicionais, nas quais há algum grau de mediação humana, o gerenciamento algorítmico nesses contextos tende a operar de forma integral, o que amplia a opacidade dos processos decisórios e limita a capacidade de compreensão e contestação por parte dos trabalhadores.

Conforme destacado por Renan Kalil (MPT) e Roseli Figaro (USP), essas relações se caracterizam pelo poder algorítmico unilateral, sem controle judicial ou administrativo efetivo sobre as decisões automatizadas.

As principais questões específicas são:

- **Decisões automatizadas sem revisão humana:** bloqueios, suspensões e descredenciamentos são aplicados por algoritmos com notificações genéricas, violando sistematicamente o art. 20 da LGPD. A decisão da Ministra Nancy Andrighi (STJ, 2023) já reconheceu a aplicação do artigo a bloqueios em plataformas, mas a prática persiste;
- **Monitoramento excessivo e invasivo:** Geolocalização contínua 24/7, reconhecimento facial para validação de identidade, análise de *rating* de usuários e geração de dados comportamentais - velocidade, trajetos, tempo de espera - sem limites claros ou finalidade específica;
- **Falta de transparência algorítmica:** O trabalhador não sabe como o algoritmo distribui demandas, calcula o preço, aplica punições ou define sua reputação;
- **Discriminação sistêmica:** Algoritmos podem excluir trabalhadores por bairro de residência, por características físicas ou por avaliações subjetivas de usuários, reproduzindo vieses raciais, de gênero e socioeconômicos. Casos documentados (ex.: iFood) mostram racismo algorítmico em sistemas de validação de identidade;
- **Assimetria informacional:** As plataformas controlam todo o fluxo de dados, e os trabalhadores não têm acesso a esses dados de forma agregada ou individualizada. O MPT tem enfrentado forte resistência das plataformas para obter dados mesmo por requisição oficial;
- **Ausência de representação coletiva:** A atomização dos trabalhadores impede a negociação coletiva sobre políticas de dados, e as plataformas resistem a qualquer forma de diálogo social.

### **7.5.1. Situações de especial vulnerabilidade: crianças e adolescentes em plataformas digitais**

Além dos trabalhadores adultos, essas dinâmicas atingem de forma ainda mais crítica grupos em situação de especial vulnerabilidade, como crianças e adolescentes inseridos em ecossistemas digitais de produção de conteúdo e monetização.

No contexto das transformações do trabalho mediadas por plataformas digitais, emerge uma zona de interseção entre trabalho infantil e tratamento intensivo de dados pessoais. A consolidação de redes sociais e plataformas como espaços de circulação econômica, produção de conteúdo e publicidade tem ampliado a presença de crianças e adolescentes em atividades que envolvem a exploração sistemática de sua imagem, de sua rotina e de seus dados comportamentais.

Destaca-se, nesse cenário, a expansão do trabalho infantil artístico no ambiente digital, especialmente associado à atuação de influenciadores mirins em plataformas digitais. Trata-se de um fenômeno caracterizado pela exposição recorrente da vida cotidiana em conteúdos frequentemente vinculados à monetização, à publicidade e a estratégias de engajamento algorítmico. Essa dinâmica intensifica riscos já identificados no trabalho artístico tradicional, ao mesmo tempo em que introduz novas dimensões relacionadas à coleta massiva de dados, ao monitoramento comportamental e à recomendação automatizada de conteúdo.

O debate jurídico no Brasil vem evoluindo para incorporar a responsabilização das plataformas digitais e a centralidade dos mecanismos de proteção integral, especialmente com base no art. 149 do Estatuto da Criança e do Adolescente (ECA), que condiciona a participação em atividades artísticas à autorização judicial. Esse entendimento foi reforçado pelo Decreto nº 12.880/2026, que atribui às plataformas deveres ativos de verificação de conformidade e remoção de conteúdos irregulares, afastando a sua caracterização como meros intermediários neutros quando participam da estruturação e monetização desses ecossistemas.

Importa destacar que nem todas as situações envolvendo crianças e adolescentes no ambiente digital se enquadram como trabalho artístico protegido. Há contextos que configuram formas proibidas de trabalho infantil, incompatíveis com o ordenamento jurídico brasileiro, nos quais os riscos associados ao tratamento de dados pessoais se somam a situações de exploração econômica e vulnerabilidade agravada. Exemplos recentes evidenciam essa realidade em diferentes setores das plataformas digitais, como a atuação de adolescentes em aplicativos de entrega, frequentemente mediante uso de contas de terceiros, em atividades marcadas por riscos físicos e ausência de proteção trabalhista, bem como a presença de adolescentes em plataformas de comercialização de conteúdo adulto, facilitada por falhas em mecanismos de verificação etária. Tais situações revelam a insuficiência de controles por parte das plataformas e a centralidade dos dados pessoais como elemento estruturante desses modelos de exploração.

Essas situações reforçam a centralidade da proteção de dados pessoais na prevenção do trabalho infantil no ambiente digital, especialmente em contextos nos quais a exploração econômica se articula ao uso intensivo de dados e à intermediação por plataformas digitais. A insuficiência dos mecanismos de aferição de idade, associada à coleta intensiva de dados e à

opacidade dos sistemas algorítmicos, contribui para a manutenção de práticas ilícitas e ampliação de riscos à privacidade, à dignidade e ao desenvolvimento de crianças e adolescentes.

Nesse cenário, o fortalecimento de mecanismos confiáveis de verificação etária e a imposição de deveres preventivos às plataformas digitais mostram-se essenciais, especialmente no que se refere à identificação de atividades ilícitas e à interrupção de modelos de exploração econômica baseados no uso intensivo de dados e da imagem de crianças e adolescentes.

As tecnologias de monitoramento e produtividade, embora possam trazer benefícios organizacionais, apresentam riscos elevados à privacidade, à não discriminação e à autodeterminação informativa dos trabalhadores. Tais riscos se intensificam no contexto da plataformização e da gestão algorítmica, em que o controle do trabalho é exercido de forma contínua, opaca e fortemente baseado na coleta e no tratamento de dados pessoais. Nesse ambiente, a exploração econômica do trabalho passa a se estruturar, de forma crescente, sobre fluxos de dados, ampliando assimetrias informacionais e reduzindo a capacidade de compreensão e contestação por parte dos trabalhadores.

Esse cenário se torna ainda mais crítico quando envolve grupos em situação de maior vulnerabilidade, como crianças e adolescentes inseridos em ecossistemas digitais de produção de conteúdo, nos quais a exploração da imagem e dos dados pessoais ocorre frequentemente sem salvaguardas adequadas. A insuficiência de mecanismos eficazes de verificação etária, associada à coleta intensiva de dados e à opacidade dos sistemas algorítmicos, contribui para a manutenção de práticas ilícitas e para a continuidade de modelos de exploração econômica baseados em dados pessoais.

A convergência entre monitoramento, inferência algorítmica e monetização de dados evidencia a necessidade de uma abordagem regulatória integrada, que articule proteção de dados pessoais, regulação do trabalho e governança de plataformas digitais. Nesse contexto, a proporcionalidade, a transparência prévia e efetiva, a limitação da coleta ao estritamente necessário, a realização de Relatório de Impacto à Proteção de Dados (RIPD) e a garantia de revisão humana de decisões automatizadas constituem requisitos indispensáveis para a conformidade com a LGPD.

Diante desse conjunto de desafios, recomenda-se a regulamentação específica do art. 20 da LGPD no contexto do trabalho mediado por plataformas digitais, estabelecendo: (i) a obrigatoriedade de supervisão humana antes de qualquer bloqueio ou suspensão; (ii) transparência acessível sobre a lógica e os critérios de decisão algorítmica; (iii) a disponibilização de canais efetivos de contestação, com prazos definidos; (iv) a vedação de monitoramento contínuo fora da “jornada”, ainda que difusa; e (v) a realização de testes de viés e avaliação de impacto para sistemas de inteligência artificial que influenciem a atividade do trabalhador. Adicionalmente, mostra-se essencial a imposição de deveres preventivos às plataformas digitais, especialmente quanto à implementação de mecanismos robustos de verificação etária, à identificação de atividades ilícitas e à interrupção de modelos de exploração econômica baseados no uso intensivo de dados e da imagem de crianças e adolescentes.

Por fim, o fenômeno da plataformização exige atuação coordenada e prioritária da ANPD em articulação com o Tribunal Superior do Trabalho, o Ministério Público do Trabalho e demais

instituições do Sistema de Garantia de Direitos, de modo a assegurar a efetividade dos direitos fundamentais dos trabalhadores e a proteção integral de crianças e adolescentes no ambiente digital.

## **8. Diálogo social e negociação coletiva no contexto da proteção de dados laboral**

A proteção de dados pessoais no contexto laboral não pode ser compreendida como um tema exclusivamente técnico, nem restrito à dimensão individual da relação entre trabalhador e empregador. Trata-se de um campo estruturado por uma assimetria de poder persistente, na qual o trabalhador possui limitações reais para compreender, contestar ou influenciar as práticas de tratamento de dados que o afetam diretamente. Nesse cenário, a efetividade dos direitos previstos na legislação depende, necessariamente, da superação dessa assimetria, o que projeta o diálogo social e a negociação coletiva como instrumentos essenciais para o reequilíbrio da relação.

Como apontado por Rafael Mosele e Martha Leal, essa assimetria assume também uma dimensão informacional, sendo estrutural no ambiente laboral, na medida em que o empregador detém o controle sobre os sistemas e tecnologias, enquanto o trabalhador experimenta seus efeitos sem plena compreensão de seus fundamentos e limites. No mesmo sentido, Carlos Fernandes Coninck Júnior ressalta que não se trata de uma relação simétrica, mas marcada por “disparidade imensa de forças”, o que restringe, na prática, a capacidade do trabalhador de recusar ou influenciar o tratamento de seus dados.

Essa realidade não apenas reforça o desequilíbrio existente, como evidencia a insuficiência de abordagens centradas exclusivamente no indivíduo, exigindo a incorporação de mecanismos coletivos capazes de viabilizar a efetividade dos direitos previstos na LGPD.

Nesse contexto, a centralidade do diálogo social decorre, em grande medida, da limitação dos instrumentos individuais para lidar com práticas complexas, opacas e de impacto coletivo. O uso crescente de tecnologias baseadas em dados, incluindo sistemas automatizados e inteligência artificial, amplia a distância entre o nível de compreensão do trabalhador e a complexidade dos tratamentos realizados, intensificando a assimetria informacional e dificultando o exercício efetivo de seus direitos.

Diante desse cenário, torna-se necessário incorporar mecanismos institucionais que permitam tratar essas questões de forma estruturada e coletiva, assegurando maior transparência, previsibilidade e capacidade de intervenção sobre práticas que, por sua natureza, ultrapassam a esfera individual e impactam coletivamente as relações de trabalho.

Essa leitura é consistente com as contribuições analisadas, que destacam que o tratamento de dados no ambiente de trabalho é contínuo, multifásico e marcado por assimetrias informacionais relevantes, o que exige respostas que ultrapassem a esfera individual e alcancem a dimensão coletiva das relações de trabalho.

A atuação coletiva permite que os trabalhadores participem, ainda que de forma indireta, da definição de limites e salvaguardas no uso de seus dados, reduzindo o risco de exposição individual e fortalecendo a capacidade de influência sobre decisões organizacionais.

O diálogo social e a negociação coletiva passam, assim, a desempenhar funções estruturantes na governança de dados no ambiente laboral, contribuindo diretamente para o equilíbrio das relações de trabalho e para a efetividade da proteção de dados.

Nesse sentido, destacam-se três dimensões principais de atuação:

- **Equilíbrio de poder**, ao reduzir a assimetria entre empregador e trabalhador e permitir que demandas sejam tratadas de forma institucional;
- **Fiscalização social**, por meio da criação de canais coletivos de controle, denúncia e mediação;
- **Concretização de direitos fundamentais**, especialmente no que se refere à privacidade, à igualdade e à não discriminação.

## **8.1 Fundamento jurídico da negociação coletiva no ordenamento brasileiro e internacional**

Importa destacar que a negociação coletiva possui fundamento consolidado no ordenamento jurídico brasileiro e internacional. No plano constitucional, o art. 7º, XXVI, da Constituição Federal reconhece as convenções e acordos coletivos de trabalho, conferindo-lhes relevância normativa, enquanto o art. 8º assegura a liberdade sindical e a autonomia das entidades representativas.

No âmbito internacional, as Convenções nº 98 e nº 154 da Organização Internacional do Trabalho reafirmam a negociação coletiva como direito fundamental e instrumento de equilíbrio nas relações laborais. Por sua vez, no direito europeu, o art. 88 do GDPR reconhece expressamente a possibilidade de utilização da negociação coletiva como mecanismo de regulação do tratamento de dados no contexto laboral, desde que asseguradas salvaguardas adequadas à proteção dos direitos e liberdades dos trabalhadores.

## **8.2 Transparência coletiva e transparência algorítmica**

Um dos elementos centrais para a efetividade da proteção de dados no ambiente laboral é o fortalecimento da transparência coletiva. Isso significa que as organizações devem adotar uma postura ativa de comunicação não apenas com os trabalhadores, mas também com seus representantes sobre práticas relevantes de tratamento de dados, especialmente aquelas que possam impactar as condições de trabalho ou a forma de organização das atividades.

Essa necessidade de ampliação da transparência - que deixa de ser apenas um dever informacional dirigido ao indivíduo e passa a incorporar uma dimensão coletiva - está diretamente relacionada ao avanço da digitalização das relações laborais. À medida que novas tecnologias são incorporadas, especialmente aquelas baseadas em dados e inteligência artificial,

torna-se essencial garantir que a informação seja compartilhada de forma prévia, estruturada e compreensível.

Como destacado nas contribuições técnicas, a transparência, nesses contextos, deve ir além da mera existência formal de informações, assegurando que trabalhadores e seus representantes compreendam não apenas que o tratamento ocorre, mas também como e com quais impactos.

A experiência internacional tem avançado no reconhecimento da negociação coletiva como instrumento legítimo de regulação do tratamento de dados no contexto laboral, inclusive com previsão expressa de participação dos representantes dos trabalhadores na definição de critérios de uso de tecnologias e proteção de direitos digitais. Nesse sentido, Caroline de Melo Gularte destaca que, em ordenamentos como o espanhol, a elaboração de políticas internas relacionadas ao uso de dispositivos digitais e monitoramento deve necessariamente contar com a participação dos representantes dos trabalhadores, reforçando a dimensão coletiva da governança de dados no trabalho.

Essa abordagem evidencia o potencial da negociação coletiva como mecanismo de concretização dos direitos fundamentais no ambiente laboral, oferecendo caminhos para o preenchimento de lacunas normativas no contexto brasileiro, nos termos do art. 8º da CLT, como bem pontuado pela Caroline de Melo Gularte.

Nesse contexto, a transparência coletiva deve assegurar visibilidade sobre aspectos centrais como:

- adoção de novas tecnologias e sistemas baseados em dados, incluindo soluções de inteligência artificial;
- mudanças nos processos produtivos e organizacionais, com potencial de alterar a dinâmica do trabalho;
- critérios gerais utilizados em sistemas automatizados, ainda que em nível explicativo;
- impactos dessas práticas sobre o trabalho e sobre os trabalhadores, inclusive em termos de organização e desempenho.

A incorporação dessas tecnologias amplia a capacidade de gestão e eficiência, mas também introduz riscos relevantes, especialmente relacionados à falta de clareza sobre como decisões são produzidas e aos efeitos indiretos que podem gerar sobre os trabalhadores.

Entre os principais riscos associados a esse cenário, destacam-se:

- opacidade decisória, dificultando a compreensão dos critérios utilizados;
- reforço de padrões e vieses existentes, a partir de dados históricos;
- impactos indiretos sobre trabalhadores, muitas vezes não evidentes de forma imediata.

Por isso, o diálogo social e a negociação coletiva devem assumir papel central para possibilitar a construção de salvaguardas que garantam maior previsibilidade e equilíbrio no tratamento de dados no contexto laboral, incluindo o uso dessas tecnologias. Esses instrumentos podem estabelecer regras claras, legitimadas e adaptadas à realidade das organizações, contribuindo para tornar operacionais os princípios da proteção de dados.

Entre os elementos mais relevantes que podem ser estruturados nesse âmbito, destacam-se:

- limites ao monitoramento, evitando práticas excessivas ou invasivas;
- tradução dessas informações em linguagem acessível ao público interno;
- avaliação prévia dos impactos sobre direitos fundamentais;
- limites ao uso de tecnologias sensíveis, como biometria e geolocalização;
- definição de critérios para decisões automatizadas, especialmente em avaliações de desempenho;
- políticas de retenção e descarte de dados;
- canais efetivos para exercício de direitos pelos trabalhadores.

Além disso, a negociação coletiva pode incorporar mecanismos mais robustos de controle e responsabilização, tais como:

- auditorias periódicas sobre o uso de dados e tecnologias;
- obrigações de prestação de contas (*accountability*);
- previsão de consequências para descumprimento das regras estabelecidas.

Diante desse cenário, a transparência não pode ser compreendida como um mero dever formal de disponibilização de informações. Mais do que isso, exige a garantia de que os conteúdos apresentados sejam inteligíveis, relevantes e efetivamente capazes de permitir aos trabalhadores compreenderem e exercerem algum nível de controle sobre o uso de seus dados pessoais. Nesse contexto, a simples apresentação de informações técnicas complexas — como códigos ou descrições altamente especializadas — revela-se insuficiente, na medida em que não assegura a compreensão real do tratamento. O que se demanda, portanto, é uma transparência substancial, capaz de traduzir, de forma clara e útil, tanto o funcionamento dos sistemas quanto os impactos concretos que produzem.

A seguir, exemplos de cláusulas que podem ser inseridas em instrumentos coletivos.

#### **CLÁUSULA 1 – TRANSPARÊNCIA NO TRATAMENTO DE DADOS**

*A empresa compromete-se a fornecer, de forma clara, acessível e prévia, aos trabalhadores e seus representantes, informações sobre o tratamento de dados pessoais no contexto laboral, incluindo: finalidades do tratamento; categorias de dados tratados; tecnologias utilizadas; compartilhamentos realizados; impactos potenciais sobre o trabalhador.*

#### **CLÁUSULA 2 – INFORMAÇÃO PRÉVIA SOBRE TECNOLOGIAS**

*A empresa deverá comunicar previamente à entidade sindical e aos trabalhadores a implementação de novas tecnologias que impliquem tratamento de dados pessoais, em especial aquelas relativas a: monitoramento; análise de desempenho; inteligência artificial; decisões automatizadas. A comunicação deverá incluir os impactos esperados sobre as condições de trabalho.*

#### **CLÁUSULA 3 – TRANSPARÊNCIA ALGORÍTMICA**

*A empresa se compromete a fornecer informações claras e compreensíveis sobre os critérios, parâmetros e lógica utilizados em sistemas automatizados que possam influenciar: avaliações de desempenho; promoção ou desligamento; distribuição de tarefas.*

#### **CLÁUSULA 4 – LIMITES AO MONITORAMENTO**

*O monitoramento de trabalhadores deverá observar: finalidade legítima e específica; proporcionalidade; limitação temporal e espacial; vedação a práticas invasivas ou discriminatórias.*

#### **CLÁUSULA 5 – CANAIS DE ATENDIMENTO**

*A empresa disponibilizará canais acessíveis e eficazes para o exercício de direitos, garantindo: confidencialidade; prazos razoáveis; ausência de retaliação.*

#### **CLÁUSULA 6 – PARTICIPAÇÃO DOS TRABALHADORES**

*Será instituída comissão paritária para acompanhamento das práticas de tratamento de dados e impactos tecnológicos no ambiente de trabalho.*

#### **CLÁUSULA 7 – AVALIAÇÃO DE IMPACTO**

*A implementação de tecnologias que envolvam tratamento de dados pessoais deverá ser precedida de avaliação de impacto, com participação ou ciência da entidade representativa dos trabalhadores.*

#### **CLÁUSULA 8 – CAPACITAÇÃO E EDUCAÇÃO**

*A empresa promoverá ações periódicas de capacitação sobre proteção de dados, com participação dos trabalhadores e de suas entidades representativas.*

### **8.3 Desafios para a efetividade da negociação coletiva no Brasil**

Na medida em que a transparência coletiva, a transparência algorítmica e os mecanismos de diálogo contínuo se consolidam como elementos centrais da governança de dados no ambiente laboral, torna-se igualmente necessário reconhecer os desafios concretos para a efetiva incorporação dessas práticas no contexto brasileiro.

Conforme destacado por Tatiana Bhering Roxo, a proteção de dados no contexto laboral ainda enfrenta entraves estruturais para sua incorporação na negociação coletiva, especialmente em razão da assimetria técnica entre as partes e da baixa maturidade sobre o tema. Nesse cenário, a negociação coletiva tende a reproduzir cláusulas genéricas, sem densidade técnica, o que limita sua capacidade de estabelecer salvaguardas efetivas no uso de dados e tecnologias no ambiente de trabalho.

Para Rafael Mosele e Martha Leal, a inserção de cláusulas coletivas voltadas à educação em proteção de dados transforma a LGPD de um tema meramente normativo em um elemento vivo

da cultura organizacional, contribuindo para reduzir assimetrias informacionais e viabilizar o exercício efetivo de direitos pelos trabalhadores.

Entre os principais entraves identificados para a efetivação da negociação coletiva, destacam-se:

- **baixa maturidade e conhecimento sobre o tema**, refletida no desconhecimento da LGPD e na limitada percepção dos riscos associados ao tratamento de dados no ambiente laboral;
- **ausência de diretrizes específicas para o contexto de trabalho**, o que leva à aplicação genérica da legislação, sem adaptação às particularidades das relações laborais;
- **assimetria técnica entre as partes**, na qual as empresas, em geral, possuem maior capacidade técnica e informacional do que os representantes dos trabalhadores;
- **barreiras culturais persistentes**, como a naturalização de práticas de vigilância e a aceitação de modelos mais invasivos de tratamento de dados.

Essa assimetria — já identificada como elemento estruturante das relações de trabalho — também se projeta sobre a capacidade de compreensão e de intervenção dos trabalhadores e seus representantes, reforçando a necessidade de mecanismos coletivos de equilíbrio. Nesse sentido, as contribuições analisadas convergem ao indicar que a proteção de dados, no contexto laboral, não pode ser tratada apenas sob uma lógica individual, devendo incorporar dimensões coletivas e institucionais de regulação.

Esses fatores contribuem para que a proteção de dados ainda não esteja plenamente integrada às agendas de negociação coletiva, dificultando a construção de soluções mais equilibradas e efetivas.

Diante desse cenário, o fortalecimento do diálogo social exige não apenas o reconhecimento desses desafios, mas a adoção de medidas estruturadas que permitam superá-los de forma progressiva e sustentável. O modelo tradicional de negociação coletiva, baseado em ciclos periódicos, mostra-se insuficiente para acompanhar a velocidade das transformações tecnológicas e organizacionais.

Nesse sentido, os caminhos apontados convergem para a necessidade de institucionalização de práticas que tornem o diálogo mais contínuo, qualificado e capaz de acompanhar a dinâmica da transformação digital, atuando de forma preventiva e não apenas reativa.

Entre as principais direções para esse fortalecimento, destaca-se:

- **institucionalização de mecanismos permanentes de diálogo**, como comissões paritárias e fóruns contínuos, capazes de acompanhar de forma estruturada os impactos tecnológicos;
- **garantia de informação prévia e qualificada**, assegurando que trabalhadores e seus representantes compreendam as tecnologias adotadas e seus efeitos;
- **investimento em capacitação técnica**, permitindo maior equilíbrio entre as partes e qualificação das negociações;

- **promoção de campanhas educativas**, voltadas à redução da assimetria informacional e ao fortalecimento da cultura de proteção de dados;
- **inclusão progressiva de cláusulas específicas nos instrumentos coletivos**, abordando temas como direitos digitais, prevenção de discriminação e definição de limites ao uso de dados.

Essa perspectiva também dialoga com as contribuições que ressaltam a centralidade da proporcionalidade, da não discriminação e da governança estruturada no tratamento de dados no trabalho, indicando que a construção de salvaguardas depende, necessariamente, de processos institucionais contínuos e informados.

Ao fortalecer a capacidade técnica, ampliar a transparência e institucionalizar espaços permanentes de diálogo - nos quais as partes acompanham continuamente os impactos da inovação tecnológica - cria-se um ambiente mais propício para que a governança de dados no trabalho seja construída de forma compartilhada, conciliando eficiência organizacional com a proteção de direitos fundamentais.

Dessa forma, a negociação coletiva não apenas complementa a legislação, mas contribui diretamente para a construção de um modelo de governança de dados mais transparente, equilibrado e eficaz no ambiente organizacional, consolidando o diálogo social como eixo estruturante da proteção de dados no contexto laboral.

## **9. Parecer Conclusivo e Subsídios Propostos**

A partir da análise das entrevistas realizadas e das contribuições escritas recebidas, o grupo buscou identificar padrões recorrentes, pontos de convergência e aspectos de maior divergência entre os diferentes setores. Esse processo permitiu a consolidação de um conjunto de entendimentos comuns, a partir dos quais foram estruturadas propostas e recomendações que podem contribuir para a atuação da Agência Nacional de Proteção de Dados.

### **9.1. Diagnóstico do Cenário Atual**

A presente análise busca examinar como a proteção de dados pessoais vem sendo aplicada no contexto das relações de trabalho, considerando as diferentes práticas, desafios e interpretações observadas nos diversos setores.

O elemento estruturante que atravessa todos os achados é a assimetria de poder e informacional nas relações de trabalho, que condiciona a aplicação da LGPD nesse contexto.

O diagnóstico consolidado a partir das entrevistas realizadas e das contribuições recebidas revela um cenário marcado por transição e elevada complexidade. Embora a Lei Geral de Proteção de Dados seja plenamente aplicável às relações laborais, sua interpretação e operacionalização ainda carecem de diretrizes específicas voltadas a esse contexto.

Essa lacuna normativa e interpretativa contribui, de um lado, para a persistência de insegurança jurídica entre empregadores, que enfrentam dificuldades na definição de parâmetros claros para o tratamento de dados, e, de outro, amplia o risco de violação de direitos dos trabalhadores, especialmente diante da ausência de critérios uniformes para aplicação da norma em situações concretas.

- **Monitoramento de Trabalhador:** Observa-se um entendimento consolidado quanto à legitimidade do monitoramento no ambiente de trabalho quando fundamentado em finalidades legítimas e claramente definidas. Contudo, há também um alerta recorrente quanto ao risco de abuso do poder diretivo, especialmente quando o tratamento de dados ultrapassa os limites da necessidade e proporcionalidade. Nesse sentido, tanto a jurisprudência trabalhista quanto diretrizes internacionais — como aquelas emitidas por autoridades europeias de proteção de dados, a exemplo da CNIL e do ICO — convergem ao apontar que práticas de monitoramento oculto, contínuo ou excessivamente invasivo tendem a ser desproporcionais. Isso inclui, entre outros, o uso de ferramentas como keyloggers, captura de tela e sistemas de geolocalização em tempo real. Diante desse cenário, a legitimidade do monitoramento está condicionada à observância de requisitos essenciais, dentre os quais se destacam a transparência prévia em relação às práticas adotadas e a escolha de meios menos invasivos para o atingimento das finalidades pretendidas. Assim, o monitoramento no contexto laboral não é vedado, mas condicionado a critérios estritos de necessidade, proporcionalidade e transparência.
- **Uso de Dados Biométricos:** a coleta de dados biométricos — especialmente para controle de jornada e gestão de acesso — configura prática recorrente nas organizações, mas envolve elevado grau de criticidade. Por se tratar de dado pessoal sensível, seu tratamento exige fundamento jurídico robusto e observância rigorosa dos princípios da necessidade e da proporcionalidade. As contribuições analisadas indicam que, embora o cumprimento de obrigação legal — como previsto no art. 74 da CLT — possa justificar a adoção de mecanismos de controle de jornada, tal fundamento não impõe, necessariamente, o uso de tecnologias biométricas. Nesse sentido, deve-se priorizar a adoção de meios menos invasivos, como crachás ou sistemas baseados em autenticação por senha, sempre que forem suficientes para atingir a finalidade pretendida. Além disso, o uso de biometria deve ser acompanhado de salvaguardas rigorosas, incluindo medidas de segurança reforçadas, transparência quanto ao tratamento e avaliação prévia de riscos. A experiência internacional, especialmente a partir de diretrizes de autoridades como a CNIL, aponta que o uso de dados biométricos deve ser tratado como exceção, e não como regra, especialmente diante do seu potencial impacto irreversível em caso de incidentes de segurança, sendo admissível apenas quando estritamente necessário e devidamente justificado.
- **Transferência Internacional de Dados:** A questão foi abordada de forma estrutural nas entrevistas realizadas com Roseli Figaro e Renan Kalil, que destacaram a predominância de grandes empresas estrangeiras de tecnologia na infraestrutura global de dados, especialmente no fornecimento de serviços de computação em nuvem e soluções de

recursos humanos. Nesse contexto, observa-se que os dados pessoais de trabalhadores brasileiros frequentemente passam a ser tratados por esses fornecedores globais, muitas vezes sem a devida avaliação de riscos ou a implementação de salvaguardas adequadas. Essa dinâmica evidencia um ponto relevante de vulnerabilidade, ao conectar a proteção de dados não apenas à esfera trabalhista, mas também a questões mais amplas de soberania digital e dependência tecnológica.

- **Exercício de Direitos dos Titulares (trabalhadores):** Observa-se, de modo geral, uma baixa efetividade prática dos direitos assegurados pela LGPD no contexto laboral. Embora existam, em muitos casos, canais formais para o exercício desses direitos, tais mecanismos tendem a ser genéricos e pouco adaptados às especificidades das relações de trabalho, o que limita sua utilização efetiva pelos trabalhadores, cenário agravado por fatores como receio de retaliação e baixa confiança nos canais institucionais. Nesse cenário, destaca-se como ponto crítico a aplicação do art. 20 da LGPD, que trata do direito à revisão de decisões automatizadas. A efetividade desse direito mostra-se particularmente desafiadora em contextos marcados por elevada opacidade algorítmica, como no trabalho mediado por plataformas digitais. Casos concretos, como os bloqueios indevidos de entregadores em plataformas — mencionados nas contribuições, com referência a situações envolvendo empresas como iFood e outras — ilustram a dificuldade de acesso à informação e de contestação das decisões automatizadas. Conforme apontado por Renan Kalil, tais situações evidenciam não apenas a limitação dos canais existentes, mas também a resistência das organizações em fornecer transparência adequada, o que compromete o exercício efetivo dos direitos pelos trabalhadores.

- **Bases Legais mais aplicáveis:**

**Consentimento:** Há amplo consenso de que o consentimento, no contexto das relações de trabalho subordinado, tende a ser inadequado e juridicamente frágil, em razão da assimetria de poder entre as partes. Seu uso indiscriminado configura uma das principais práticas equivocadas identificadas no tratamento de dados pessoais no ambiente laboral. Nesse sentido, o consentimento deve ser tratado como medida excepcional, restrita a situações verdadeiramente facultativas — como a participação em programas de bem-estar ou o uso de imagem para finalidades não essenciais —, sendo admissível apenas quando houver comprovação efetiva de que a recusa não acarretará qualquer tipo de prejuízo ao trabalhador.

**Legítimo Interesse:** Trata-se de uma base legal central, porém de aplicação complexa no contexto laboral. As contribuições analisadas — com destaque para os apontamentos de Caroline Melo e Ana Rita Biba — convergem no sentido de que sua utilização exige a realização de um teste de balanceamento rigoroso e devidamente documentado (Legitimate Interest Assessment – LIA), acompanhado da adoção de salvaguardas adicionais e de um nível reforçado de transparência. Nesse sentido, o legítimo interesse

não pode ser aplicado de forma genérica ou presumida, devendo estar sempre fundamentado em análise concreta que demonstre sua adequação, necessidade e proporcionalidade frente aos direitos e liberdades dos trabalhadores.

**Execução de Contrato e Obrigação Legal:** Essas bases legais constituem, em regra, os fundamentos mais robustos e amplamente utilizados para a maioria das operações de recursos humanos, como folha de pagamento, cumprimento de obrigações trabalhistas e envio de informações a sistemas oficiais, a exemplo do eSocial. No entanto, o diagnóstico evidencia um risco recorrente de utilização excessivamente ampla e imprecisa dessas hipóteses, como se funcionassem como autorizações genéricas para o tratamento de dados.

Nesse contexto, torna-se essencial delimitar com clareza quais operações são estritamente necessárias para o cumprimento da obrigação legal ou da execução contratual, evitando interpretações extensivas que ampliem indevidamente o escopo do tratamento.

## 9.2. Convergências e Tensões Identificadas

Pontos de alinhamento e conflito entre os direitos à privacidade e proteção de dados e interesses legítimos do empregador.

- **Convergências:**

**Vulnerabilidade do Trabalhador:** Existe convergência entre todos os entrevistados quanto à importância de evitar esforços para uma correta aplicação da LGPD no contexto laboral para que a assimetria de poder, inerente à relação de trabalho, não se some à assimetria informacional, vulnerabilizando ainda mais o trabalhador.

**Centralidade dos Princípios:** Há um alinhamento sobre a importância dos princípios da finalidade, necessidade e transparência como balizas fundamentais para qualquer tratamento de dados.

**Excepcionalidade do Consentimento:** É ponto pacífico que o consentimento não deve ser a base legal prioritária no contexto laboral.

**Necessidade de Transparência Ativa:** Todos reconhecem que a transparência é o principal mecanismo de legitimidade e prevenção de abusos no tratamento de dados dos trabalhadores.

Esses pontos de convergência indicam a formação de um núcleo comum de entendimento sobre a aplicação da LGPD no contexto laboral, especialmente orientado pelos princípios da transparência, necessidade e proteção da parte vulnerável.

- **Tensões:**

**Alcance do Poder Diretivo vs. Privacidade:** Há um embate sobre os limites do monitoramento. De um lado, há quem defenda a legitimidade do monitoramento como inerente ao poder diretivo e à proteção patrimonial. De outro, os que defendem uma aplicação estrita dos princípios da necessidade e proporcionalidade, vedando práticas

invasivas e exigindo a escolha da alternativa menos intrusiva. A discussão sobre o uso de geolocalização e *boss ware* exemplifica essa tensão.

**Negociação Coletiva como Instrumento Regulatório:** um dos pontos de maior tensão identificados diz respeito ao papel da negociação coletiva na regulação da proteção de dados no contexto laboral. De um lado, há entendimento de que a negociação coletiva constitui instrumento fundamental para detalhar regras, estabelecer salvaguardas e viabilizar a efetivação de direitos. De outro, há posições que ressaltam que a proteção de dados, por se tratar de direito fundamental, possui caráter indisponível, não podendo ser objeto de flexibilização por meio de negociação coletiva.

Essa tensão se reflete, inclusive, na jurisprudência recente, como em decisão do Tribunal Superior do Trabalho que declarou inválida cláusula coletiva que previa o compartilhamento compulsório de dados pessoais de empregados com entidades sindicais.

Diante desse cenário, evidencia-se que a negociação coletiva deve ser compreendida como instrumento de regulação e aprimoramento da proteção de dados no ambiente de trabalho, voltado à criação de regras específicas que assegurem transparência, governança e proteção dos trabalhadores. Nesse sentido, não deve ser visto como um instrumento de flexibilização, mas de densificação e concretização de direitos.

**Soft Law vs. Hard Law:** De modo geral, observa-se que o setor produtivo tende a defender a adoção de orientações de caráter não vinculante — como guias e recomendações —, sob o argumento de que abordagens excessivamente prescritivas podem restringir a capacidade de gestão e limitar a inovação. Em contraposição, as demais contribuições apontam para a necessidade de maior clareza normativa, especialmente em temas mais sensíveis, como o uso de decisões automatizadas, nos termos do art. 20 da LGPD, e o tratamento de dados biométricos.

Esse contraste evidencia uma tensão entre flexibilidade regulatória e segurança jurídica, indicando a necessidade de construção de parâmetros que, ao mesmo tempo, garantam proteção efetiva aos trabalhadores e ofereçam previsibilidade para as organizações.

De modo geral, o setor produtivo defende que as orientações sobre o tema devem ser não vinculantes (guias, recomendações), temendo que regras prescritivas engessem a gestão e a inovação. Em contraste, os demais setores apontam para a necessidade de regras mais claras, especialmente sobre temas como decisões automatizadas (art. 20) e uso de biometria.

### 9.3. Propostas de abordagens

As propostas a seguir buscam responder diretamente aos desafios identificados no diagnóstico, especialmente aqueles relacionados à assimetria informacional, à ausência de diretrizes específicas e à crescente complexidade tecnológica.

- **Boas práticas para coleta e tratamento de dados de trabalhadores:** a definição de diretrizes para o tratamento de dados no contexto laboral deve adotar uma abordagem estruturada, alinhada às diferentes fases da relação de trabalho e aos riscos associados a cada uma delas. Nesse sentido, destacam-se as seguintes orientações:
- **Governança por fases:** recomenda-se que o tratamento de dados seja orientado a partir do ciclo de vida da relação laboral — pré-contratual, contratual e pós-contratual —, de modo a assegurar maior aderência às finalidades e às bases legais aplicáveis em cada etapa.
- **Minimização de dados:** a coleta deve observar a lógica do *just in time* e *just enough*, evitando práticas baseadas na coleta preventiva (*just in case*). Nesse contexto, a coleta de informações relacionadas à saúde — como a indicação de CID em atestados —, antecedentes criminais ou dados de crédito deve ser considerada legítima apenas em hipóteses excepcionais, devidamente justificadas e amparadas em base legal adequada.
- **Avaliação de necessidade e proporcionalidade:** para o uso de tecnologias mais intrusivas, como ferramentas de monitoramento e que tratam dados biométricos, deve-se exigir a realização prévia de avaliação que demonstre, de forma concreta, a necessidade do tratamento e a inexistência de meios menos invasivos para o atingimento da finalidade pretendida, reforçando a obrigação de escolha da alternativa que melhor concilie eficiência operacional e proteção dos direitos dos trabalhadores.
- **Transparência e Consentimento no Contexto Laboral:**
  - a. **Avisos de privacidade específicos:** recomenda-se a elaboração de avisos de privacidade direcionados ao público interno, estruturados de forma segmentada e com linguagem clara e acessível, evitando excesso de tecnicidade. Sempre que possível, deve-se adotar formatos em camadas (*layered notices*), que facilitem a compreensão progressiva das informações, bem como garantir sua disponibilização em canais de fácil acesso, como intranet corporativa e recursos digitais (ex.: QR Codes).
  - b. **Fragilidade do consentimento:** é fundamental que diretrizes institucionais reconheçam a fragilidade do consentimento no contexto laboral, presumindo-se sua limitação em razão da assimetria de poder existente. Sua aplicação deve ser restrita a situações efetivamente opcionais, nas quais a recusa não acarrete qualquer prejuízo ao trabalhador.
  - c. **Transparência ativa:** a transparência não deve ser compreendida como um dever passivo, restrito à disponibilização de informações. Ao contrário, recomenda-se a adoção de práticas de comunicação ativa, especialmente em

relação a alterações nos avisos de privacidade e à implementação de novas tecnologias no ambiente de trabalho, de modo a assegurar que os trabalhadores sejam informados de forma clara, tempestiva e compreensível sobre mudanças relevantes no tratamento de seus dados.

- **Políticas de Retenção de Dados:**

- a. **Prazos Variáveis:** recomenda-se esclarecer que não existe um prazo único e uniforme para retenção de dados pessoais no contexto laboral. Os períodos de armazenamento devem ser definidos a partir das diferentes finalidades do tratamento e das obrigações legais aplicáveis, incluindo, entre outros, prazos de natureza trabalhista, previdenciária e fiscal, evitando tanto a retenção excessiva quanto a eliminação prematura de dados necessários.
- b. **Pseudonimização como salvaguarda:** recomenda-se a adoção de técnicas de pseudonimização como medida de proteção adicional, especialmente para dados mantidos por períodos prolongados, como aqueles necessários para fins de defesa judicial. Nesses casos, o acesso a informações que permitam a identificação direta do trabalhador deve ser restrito ao estritamente necessário, reforçando os mecanismos de segurança e controle sobre o tratamento.

- **Uso de Tecnologias de Monitoramento e Decisões Automatizadas:**

- a. **Direito à Explicação e Revisão Humana:** orientar a aplicação do art. 20 da LGPD no contexto laboral, assegurando que decisões automatizadas que produzam efeitos relevantes — como seleção, avaliação, promoção ou desligamento — sejam passíveis de revisão humana qualificada. Além disso, garantir a disponibilização de informações claras sobre os critérios gerais utilizados, preservados eventuais segredos comerciais.
- b. **Avaliação de impacto à proteção de dados (RIPD):** orientar a necessidade de elaboração de Relatório de Impacto à Proteção de Dados para o uso de tecnologias classificadas como de alto risco, incluindo sistemas de reconhecimento facial, ferramentas de monitoramento contínuo de produtividade e algoritmos aplicados à gestão de pessoas. Esse instrumento é essencial para identificar riscos, avaliar proporcionalidade e definir salvaguardas adequadas.
- c. **Vedação ao uso secundário de dados:** orientar que a reutilização de dados coletados para uma finalidade específica — como controle de acesso — para finalidades distintas e incompatíveis — como avaliação de desempenho — configura desvio de finalidade. Nessas hipóteses, o tratamento deve ser considerado vedado, salvo quando houver nova base legal

adequada e garantia de transparência aos titulares.

- **Governança e Accountability nas Empresas:**

- a. **Papel do DPO:** Orientar o fortalecimento do papel do Encarregado como elemento central na governança de dados, atuando como ponte entre a organização e os trabalhadores. Para tanto, ressaltar a importância de assegurar sua autonomia técnica, bem como o acesso direto à alta gestão, de modo a garantir a efetividade de sua atuação na orientação, monitoramento e supervisão das práticas de tratamento de dados.
- b. **Documentação Obrigatória:** orientar quanto a importância do Registro de Operações de Tratamento (ROT) como instrumento fundamental de governança e accountability. Recomenda-se que a Agência Nacional de Proteção de Dados incentive a elaboração de registros específicos para a área de recursos humanos, com detalhamento das finalidades, bases legais utilizadas e, quando aplicável, dos testes de balanceamento (LIA), contribuindo para maior transparência e rastreabilidade das decisões.
- c. **Gestão de Terceiros:** orientar a adoção de processos estruturados de *due diligence* na contratação de fornecedores, especialmente aqueles responsáveis por tecnologias de RH e tratamento de dados. É fundamental que esses parceiros estejam em conformidade com a LGPD e que as salvaguardas de proteção de dados sejam expressamente previstas em contrato, incluindo cláusulas de segurança, limitação de finalidade e responsabilidades em caso de incidentes.

#### 9.4. Recomendações para Ações Futuras

Temas que merecem aprofundamento, possíveis resoluções e campanhas de orientação.

1. **Aprofundamento Temático:** considerando a complexidade e a evolução contínua das relações de trabalho mediadas por dados e tecnologias, recomenda-se o desenvolvimento de análises específicas sobre temas que apresentam maior grau de criticidade e urgência regulatória. Nesse sentido, destacam-se as seguintes frentes de aprofundamento:
  - a. **Trabalho em Plataformas:** recomenda-se o desenvolvimento de estudos específicos voltados à proteção de dados de trabalhadores vinculados a plataformas digitais, como motoristas e entregadores, com foco na gestão algorítmica, nos mecanismos de bloqueio automatizado e na efetivação do direito previsto no art. 20 da LGPD. Nesse contexto, a articulação institucional com o Ministério Público do Trabalho revela-se estratégica para o avanço da regulação e da fiscalização.

- b. **Proteção de Crianças e Adolescentes:** destaca-se a necessidade de elaboração de diretrizes específicas para o tratamento de dados de aprendizes e de crianças e adolescentes que atuam em ambientes digitais, como influenciadores mirins. Essas diretrizes devem observar o princípio da proteção integral e do melhor interesse da criança, incorporando abordagem baseada em risco e prevendo salvaguardas proporcionais à exposição e à complexidade do ambiente digital. Nesse contexto, recomenda-se atenção especial a lacunas de controle em atividades mediadas por plataformas digitais, como a participação de menores em aplicativos e ecossistemas digitais de monetização, bem como aos riscos associados ao trabalho infantil artístico, ao uso intensivo de dados comportamentais e à exploração econômica da imagem. Destaca-se, ainda, a necessidade de fortalecimento de mecanismos confiáveis de verificação etária e de deveres preventivos por parte das plataformas digitais, incluindo a identificação de práticas ilícitas e a interrupção de fluxos econômicos baseados no uso de dados pessoais de crianças e adolescentes, em consonância com os princípios da LGPD e com o sistema de proteção integral.
- c. **Transferência Internacional de Dados:** recomenda-se a promoção de estudos voltados à análise dos fluxos internacionais de dados de trabalhadores, especialmente no contexto de dependência de fornecedores globais de tecnologia. Esses estudos devem considerar os riscos associados à soberania digital, à concentração de infraestrutura em grandes empresas transnacionais e à necessidade de estabelecimento de salvaguardas adequadas para essas transferências.
- d. **Inteligência Artificial no Trabalho:** destaca-se a importância de aprofundar a análise sobre o uso de ferramentas de inteligência artificial em processos de recrutamento e gestão de pessoas, com foco nos riscos de vieses discriminatórios. Nesse sentido, recomenda-se o desenvolvimento de diretrizes voltadas à auditoria algorítmica, à transparência e à mitigação de riscos associados a decisões automatizadas.
- e. **Datificação do Trabalho:** recomenda-se o fortalecimento de iniciativas de fiscalização e pesquisa voltadas à compreensão de como, em que medida e com quais finalidades dados da atividade laboral vêm sendo gerados e utilizados por plataformas e serviços digitais. Esse aprofundamento deve considerar o uso desses dados para automação de processos, melhoria de produtos e treinamento de sistemas de inteligência artificial, contribuindo para maior transparência e controle sobre essas práticas.

## 2. Possíveis Resoluções e Guias:

- a. **Guia Orientativo sobre Monitoramento Laboral:** recomenda-se a elaboração de guia específico que aborde, de forma prática, o uso de tecnologias de monitoramento no ambiente de trabalho, incluindo estudos de caso sobre videomonitoramento, geolocalização, softwares de produtividade e datificação da atividade laboral. O objetivo é estabelecer parâmetros claros de necessidade e proporcionalidade.
  - b. **Resolução sobre Decisões Automatizadas:** sugere-se a edição de orientação normativa voltada à aplicação do art. 20 da LGPD no contexto laboral, com definição mais precisa sobre o que caracteriza “intervenção humana significativa”, bem como sobre as informações mínimas que devem ser disponibilizadas aos trabalhadores, com atenção especial às situações envolvendo trabalhadores plataformizados.
  - c. **Guia sobre Negociação Coletiva:** recomenda-se a elaboração de guia orientativo que esclareça a interface entre a proteção de dados pessoais e a negociação coletiva no contexto laboral, delimitando os temas passíveis de regulamentação por instrumentos coletivos e distinguindo aqueles que, por envolverem direitos fundamentais, não admitem flexibilização. O guia deve oferecer diretrizes práticas para a elaboração de cláusulas compatíveis com a LGPD, com ênfase nos princípios da finalidade, necessidade, transparência e não discriminação, bem como orientar a incorporação de mecanismos de governança, transparência ativa, canais efetivos de exercício de direitos e iniciativas de capacitação no ambiente de trabalho. Nesse sentido, a negociação coletiva deve ser compreendida como instrumento de concretização dos direitos dos trabalhadores enquanto titulares de dados, e não de sua flexibilização.
- 3. Campanhas de Orientação e Capacitação:** Recomenda-se o fortalecimento de iniciativas estruturadas de capacitação e educação em proteção de dados pessoais no contexto laboral, compreendidas como instrumento essencial para a redução de assimetrias informacionais e para a efetivação dos direitos dos trabalhadores enquanto titulares de dados. A recorrência de práticas como coleta excessiva de dados, uso inadequado de bases legais, monitoramento desproporcional e baixa transparência evidencia que a insuficiência de cultura organizacional e de capacitação técnica constitui fator estruturante de risco nas relações de trabalho mediadas por dados e tecnologias. Nesse sentido, a promoção de uma cultura de proteção de dados mostra-se indispensável para a aplicação efetiva dos princípios da finalidade, necessidade, proporcionalidade e transparência previstos na LGPD.
- a. **Campanha para Trabalhadores:** propõe-se o desenvolvimento de iniciativas educativas contínuas e acessíveis, voltadas à conscientização

dos trabalhadores sobre o tratamento de seus dados pessoais no ambiente laboral. Essas iniciativas devem abordar, de forma clara e didática, o funcionamento das tecnologias de monitoramento, os dados coletados no exercício da atividade profissional, os critérios utilizados em sistemas automatizados e os mecanismos disponíveis para o exercício de direitos, como acesso, revisão e contestação. Tais ações são fundamentais para reduzir assimetrias informacionais estruturais e permitir o exercício efetivo da autodeterminação informativa, especialmente em contextos de crescente automação e uso de inteligência artificial na gestão do trabalho.

- b. **Capacitação para RH e DPOs:** recomenda-se a implementação de programas estruturados de capacitação técnica voltados às áreas de recursos humanos e às lideranças organizacionais, com foco na aplicação adequada da LGPD no contexto das relações de trabalho. Esses programas devem contemplar temas como definição de bases legais, limitação da coleta de dados, governança de dados no RH, prevenção de práticas discriminatórias, uso proporcional de tecnologias de monitoramento e gestão de riscos associados a decisões automatizadas. Considerando que o setor de recursos humanos concentra parcela significativa das operações de tratamento de dados pessoais, sua adequada capacitação constitui elemento central para a prevenção de infrações legais e para o fortalecimento da conformidade organizacional.
- c. **Capacitação sobre proteção de dados de crianças e adolescentes:** recomenda-se o desenvolvimento de ações formativas específicas voltadas à sensibilização de agentes públicos e privados quanto aos riscos associados ao tratamento de dados pessoais de crianças e adolescentes em ambientes digitais. Essas iniciativas devem abordar aspectos como verificação etária, exploração econômica da imagem, uso de dados em plataformas digitais e riscos associados à monetização de conteúdo, especialmente no caso de influenciadores mirins. A capacitação nesse campo mostra-se essencial para a efetivação do princípio da proteção integral e para a prevenção de práticas abusivas no ambiente digital.

- 4. **Fluxo de Testes de Plataformas e Serviços Digitais:** considerando a crescente dependência de soluções tecnológicas no contexto laboral, recomenda-se a avaliação da viabilidade de adoção de um modelo estruturado de verificação técnica de softwares utilizados em relações de trabalho, como sistemas de recursos humanos, plataformas digitais e ferramentas de monitoramento. Nesse sentido, propõe-se a implementação de um processo de verificação que contemple etapas progressivas de análise, incluindo:

- a) **Verificação documental:** análise inicial da documentação técnica da ferramenta, com foco nas finalidades do tratamento, bases legais, fluxos de dados e medidas de segurança declaradas.
- b) **Testes técnicos automatizados:** realização de testes voltados à identificação de riscos, incluindo mapeamento dos dados gerados, análise de tráfego para identificação de controladores e destinatários, verificação de vulnerabilidades e avaliação de permissões excessivas.
- c) **Classificação de risco:** a partir dos resultados obtidos, recomenda-se a utilização de mecanismos automatizados de classificação que categorizarão as ferramentas em níveis de risco (baixo, médio ou alto), considerando a natureza dos dados tratados e os potenciais impactos sobre os titulares. Ferramentas classificadas como de maior risco devem ser submetidas a análise humana aprofundada.

Como resultado desse processo, sugere-se a geração de um manifesto digital de transparência, que poderá ser incorporado ao próprio código da ferramenta ou disponibilizado publicamente, contendo informações essenciais como:

- nível de risco atribuído
- tipos de dados coletados
- destinatários dos dados
- medidas de segurança adotadas
- prazo de validade da avaliação

Esse manifesto poderá ser objeto de certificação ou assinatura institucional pela ANPD, com o objetivo de garantir sua autenticidade e confiabilidade. Recomenda-se, ainda, que tais informações sejam disponibilizadas de forma acessível aos usuários — por exemplo, por meio de interfaces específicas (“Transparência LGPD”) ou integração via API.

O modelo proposto apresenta potencial para promover maior transparência, escalabilidade e conformidade proativa com a LGPD, ao mesmo tempo em que permite equilibrar automação e supervisão humana, de acordo com o nível de risco das operações de tratamento realizadas.

## 10. Conclusão

A análise aprofundada das entrevistas realizadas e dos documentos que compõem o presente relatório evidencia um cenário marcado pela diversidade de perspectivas, mas também por elevada complexidade. Nesse contexto, a proteção de dados pessoais nas relações de trabalho consolida-se como um dos temas mais desafiadores da atualidade. A síntese das contribuições oriundas de especialistas aponta para a necessidade de uma abordagem que ultrapasse a aplicação estritamente literal da LGPD, demandando a construção de diretrizes específicas, proporcionais e aderentes às particularidades do contexto laboral brasileiro.



As contribuições analisadas convergem para a premissa de que o tratamento de dados no ambiente de trabalho não se desenvolve em condições de simetria entre as partes. A vulnerabilidade estrutural do trabalhador — independentemente do tipo de vínculo, seja celetista, autônomo ou plataformizado — foi reiteradamente destacada como elemento central, exigindo maior rigor na aplicação dos princípios da finalidade, necessidade e transparência. Nesse sentido, especialistas como Ana Rita Biba, Selma Carlotto, Caroline Melo e Priscila Zoghbi, entre outros, apontam de forma convergente que o consentimento, em regra, apresenta fragilidade significativa nesse contexto, devendo ser substituído por hipóteses legais mais adequadas, como a execução de contrato e o cumprimento de obrigação legal, desde que delimitadas de forma estrita e devidamente justificadas.

Na sequência, evidencia-se a existência de tensões relevantes entre a proteção de direitos fundamentais dos trabalhadores e os interesses legítimos das organizações, especialmente no que se refere ao uso de tecnologias e ao monitoramento das atividades laborais. Enquanto representantes do setor produtivo enfatizam o poder diretivo do empregador e a necessidade de segurança jurídica para a gestão, outras contribuições alertam para os riscos associados à vigilância excessiva, à discriminação algorítmica e ao uso indevido ou secundário de dados pessoais. Casos concretos mencionados nas contribuições, como bloqueios automatizados de trabalhadores em plataformas digitais, ilustram de forma clara como a ausência de transparência e de mecanismos efetivos de revisão humana pode resultar em violações de direitos fundamentais.

Destaca-se, ainda, que os desafios relacionados à proteção de dados no contexto do trabalho mediado por plataformas digitais assumem contornos ainda mais críticos quando envolvem crianças e adolescentes inseridos em ecossistemas digitais de produção de conteúdo e monetização. Nesses casos, a exploração econômica da imagem e dos dados pessoais se articula a dinâmicas algorítmicas e a insuficiências em mecanismos de verificação etária, ampliando riscos à privacidade, à dignidade e ao pleno desenvolvimento desses titulares. Tal cenário reforça a necessidade de fortalecimento de deveres preventivos por parte das plataformas digitais, bem como de uma abordagem regulatória integrada, capaz de articular proteção de dados pessoais, direitos da infância e regulação do trabalho.

Em continuidade, o papel do diálogo social e da participação coletiva emerge como um dos pontos mais sensíveis e debatidos. De um lado, experiências comparadas e contribuições específicas indicam que a negociação coletiva pode constituir instrumento relevante para detalhar e operacionalizar regras de proteção de dados no ambiente de trabalho. De outro, há posicionamentos que ressaltam que a proteção de dados, por se tratar de direito fundamental, possui caráter indisponível, não podendo ser objeto de flexibilização por meio de negociação coletiva.

Essa tensão se reflete, inclusive, na jurisprudência recente, como em decisão do Tribunal Superior do Trabalho que declarou inválida cláusula coletiva que previa o compartilhamento compulsório de dados pessoais de empregados com entidades sindicais.

Diante desse cenário, consolida-se o entendimento de que a negociação coletiva deve ser compreendida não como instrumento de flexibilização de direitos, mas como mecanismo de sua densificação e concretização no contexto laboral. Sua função, nesse sentido, consiste em traduzir os princípios da LGPD em regras operacionais, adaptadas às especificidades dos setores e das organizações, contribuindo para a redução das assimetrias informacionais e para o fortalecimento da governança de dados no trabalho.



Assim, a atuação dos instrumentos coletivos deve observar, como limite inafastável, a vedação à redução de direitos fundamentais, ao mesmo tempo em que se apresenta como via legítima para sua ampliação, operacionalização e efetividade, especialmente em contextos marcados por elevada complexidade tecnológica e por impactos coletivos das práticas de tratamento de dados.

Por fim, verifica-se uma convergência relevante entre os diferentes atores quanto ao papel da ANPD como agente indutor de boas práticas, especialmente por meio da elaboração de guias orientativos, estudos de caso e iniciativas de capacitação. Em geral, observa-se preferência por instrumentos flexíveis e orientativos, capazes de oferecer segurança jurídica sem comprometer a inovação. Nesse contexto, a proposta de elaboração de guias estruturados a partir de problemas concretos e organizados segundo as fases da relação laboral foi amplamente reconhecida como abordagem adequada para promover a efetividade dos direitos dos trabalhadores e a conformidade por parte das organizações.

Destaca-se, ainda, que a efetividade das diretrizes propostas não depende exclusivamente da atuação normativa da ANPD, mas também do fortalecimento de iniciativas estruturadas de capacitação e educação em proteção de dados no contexto laboral. A recorrente assimetria informacional entre empregadores e trabalhadores, aliada à crescente complexidade das tecnologias utilizadas na gestão do trabalho, evidencia que a compreensão efetiva sobre o funcionamento do tratamento de dados pessoais constitui condição essencial para o exercício de direitos e para a legitimidade dessas práticas. Nesse sentido, ações contínuas de capacitação, campanhas de orientação e formação técnica de agentes públicos e privados mostram-se fundamentais para promover uma cultura de proteção de dados no ambiente de trabalho. Esse desafio assume contornos ainda mais sensíveis nos casos que envolvem crianças e adolescentes em ambientes digitais, exigindo abordagens formativas específicas e alinhadas ao princípio da proteção integral.

Dessa forma, o presente relatório consolida o entendimento de que a proteção de dados no contexto laboral não constitui um tema periférico, mas um eixo estruturante para a construção de um ambiente de trabalho digital que seja justo, transparente e compatível com a dignidade da pessoa humana. Nesse contexto, destaca-se que a efetividade desse modelo demanda não apenas a observância formal das normas, mas também o fortalecimento de mecanismos de transparência ativa, capazes de assegurar que os trabalhadores compreendam de forma clara o tratamento de seus dados pessoais, bem como a disponibilização de canais acessíveis, eficazes e seguros para o exercício de seus direitos enquanto titulares.

As recomendações aqui apresentadas, fundamentadas nas contribuições e experiências analisadas no âmbito deste grupo de trabalho do CNPD, buscam contribuir para que a atuação da ANPD promova um equilíbrio adequado entre inovação, eficiência econômica e a efetiva salvaguarda dos direitos fundamentais das pessoas trabalhadoras, assegurando não apenas a conformidade regulatória, mas também a legitimidade social das práticas de tratamento de dados no ambiente de trabalho.

## **11. Anexos**

1. Ata de instituição do GT (Portaria CNPD nº 01/2025);
2. Plano de trabalho aprovado;

3. Atas das reuniões realizadas;
4. Registro das entrevistas com especialistas e entidades;
5. Drive com as contribuições recebidas

### **Anexo 1 – Portaria de instituição do GT**



## CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

PORTARIA CNPD Nº 01, DE 05 DE NOVEMBRO DE 2025

Institui Grupo de Trabalho dedicado a proposições, na temática da Proteção de Dados no Contexto Laboral, no âmbito do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

O PRESIDENTE SUBSTITUTO DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE - CNPD, no uso das atribuições que lhe conferem os arts. 14, 15, 16 e 17 do Anexo I ao Decreto nº 10.474, de 26 de agosto de 2020, os arts. 24, 25, 26, 27, 28 e 29 da Resolução CNPD nº 2, de 26 de setembro de 2024, considerando o disposto no art. 58-B da Lei nº 13.709 de 14 de agosto de 2018 e considerando a deliberação adotada na 1ª (primeira) reunião extraordinária do CNPD, **RESOLVE**:

Art. 1º Esta Portaria institui, no âmbito do Conselho Nacional de Proteção de Dados e da Privacidade - CNPD, Grupo de Trabalho dedicado a proposições, na temática da Proteção de Dados no Contexto Laboral.

Art. 2º Compete ao Grupo de Trabalho realizar análises, estudos e fazer proposições na temática da Proteção de Dados no Contexto Laboral.

Art. 3º O Grupo de Trabalho é composto pelos seguintes membros do CNPD:

I - Débora Sirotheau Siqueira Rodrigues, membro titular representante de entidades representativas do Setor Laboral, que o coordenará;

II - Alexandre Zago Boava, membro titular representante de entidades representativas do Setor Laboral;

III - Cassio Augusto Muniz Borges, membro titular representante de Confederações Sindicais representativas das categorias econômicas do setor produtivo;

IV - Gabrielle Bezerra Sales Sarlet, membro titular representante de Instituições científicas, tecnológicas e de inovação;

V - Isabella Vieira Machado Henriques, membro titular representante de Organizações da Sociedade Civil com atuação comprovada em proteção de dados pessoais; e

VI - João Marcos Pereira Vidal, membro suplente representante de entidades representativas do Setor Laboral.

§ 1º O coordenador do Grupo de Trabalho indicará um suplente, que o substituirá em suas ausências e impedimentos.

§ 2º Os membros do Grupo de Trabalho devem assegurar o cumprimento das atividades estabelecidas nos prazos determinados e responder tempestivamente às demandas recebidas.

Art. 4º O coordenador apresentará plano de trabalho contendo o planejamento das atividades a serem desenvolvidas pelo colegiado em até trinta dias da entrada em vigor desta Portaria.

Parágrafo único. O plano de trabalho referido no *caput* deverá conter calendário das reuniões do Colegiado.

Art. 5º As reuniões serão convocadas pelo coordenador com, no mínimo, sete dias de antecedência.

§ 1º As reuniões do Grupo de Trabalho serão realizadas, preferencialmente, por videoconferência.

§ 2º O quórum das reuniões do Grupo de Trabalho é de maioria simples de seus membros.

§ 3º As deliberações do Grupo de Trabalho serão aprovadas pela maioria simples dos membros presentes, nos casos de deliberações em reuniões ou pela maioria absoluta dos membros, nos casos de deliberação por meio eletrônico.

§ 4º O coordenador do grupo atuará também como relator e estabelecerá os procedimentos para manifestação dos presentes nas reuniões.

§ 5º Caberá ao coordenador do grupo o envio do convite e da pauta das reuniões do Grupo de Trabalho, por correspondência eletrônica, aos participantes, bem como elaborar as atas das reuniões, expedientes e

pareceres, encaminhando-os à Secretaria-Geral para fins de arquivo.

§ 6º O coordenador do Grupo de Trabalho deverá informar, em todas as reuniões do CNPD, o andamento das atividades desenvolvidas pelo grupo e os principais encaminhamentos realizados.

§ 7º O Grupo de Trabalho poderá se reunir com os grupos de trabalho de outros colegiados para a realização de discussão integrada de matérias de interesse do CNPD.

§ 8º O coordenador dos Grupo de Trabalho poderá convidar demais membros do CNPD e especialistas para colaborar com as atividades do grupo, sem remuneração e sem direito à voto.

Art. 6º A proposição elaborada pelo Grupo de Trabalho deverá ser apresentada sob a forma de relatório final, que deverá ser assinado pelo seu relator e conter, no mínimo:

I - o histórico das atividades desenvolvidas;

II - os produtos elaborados; e

III - o parecer conclusivo sobre o fornecimento de subsídios na temática objeto de estudo pelo Grupo de Trabalho.

Art. 7º O Grupo de Trabalho apresentará relatório final em até cinco dias após o término do prazo de suas atividades.

Parágrafo único. O relatório final de que trata o *caput* será submetido à deliberação do CNPD.

Art. 8º O Grupo de Trabalho terá duração de cento e vinte dias a contar da data de entrada em vigor desta Portaria, podendo ser prorrogado por igual período mediante solicitação justificada de seu coordenador à Presidência do CNPD.

Art. 9º A participação no Grupo de Trabalho será considerada prestação de serviço público relevante, não remunerada.

Art. 10. Aplicam-se às normas dispostas nesta Portaria as disposições previstas no Regimento Interno do CNPD que dizem respeito aos Grupos de Trabalho.

Parágrafo único. As situações afetas ao Grupo de Trabalho não previstas nesta Portaria ou no Regimento Interno do CNPD serão tratadas pelo Coordenador do Grupo de Trabalho e decididas pela Presidência do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Art. 11. Esta Portaria entra em vigor na data de sua publicação.

**VICTOR EPITACIO CRAVO TEIXEIRA**

Presidente do Conselho substituto



Documento assinado eletronicamente por **Victor Epitácio Cravo Teixeira, Usuário Externo**, em 05/11/2025, às 17:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0213865** e o código CRC **DEDB9130**.

SCN Quadra 06, Ed. Venâncio 3000, Bloco A, 9º andar - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2017-3338 / 3339 - <https://www.gov.br/anpd/pt-br>

Referência: Processo nº 00261.006039/2024-45

SEI nº 0213865

## Anexo 2 – Plano de Trabalho Aprovado



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE  
(CNPd)  
GRUPO DE TRABALHO 1- PROTEÇÃO DE DADOS NO CONTEXTO LABORAL  
PLANO DE TRABALHO**

**Coordenadora:** Débora Sirotheau

**Vice-Coordenador (a):** (a definir pelo GT)

**Composição do GT:**

- Débora Sirotheau Siqueira Rodrigues
- Alexandre Zago Boava
- Cassio Augusto Muniz Borges
- Gabrielle Bezerra Sales Srlet
- Isabella Vieira Machado Henriques
- João Marcos Pereira Vidal

**I. OBJETIVO GERAL:**

Realizar análises, estudos e proposições na temática da Proteção de Dados no Contexto Laboral, fornecendo subsídios técnicos para a atuação da Agência Nacional de Proteção de Dados (ANPD) na aplicação da LGPD no contexto laboral, fortalecendo a proteção de dados de trabalhadores e fornecendo segurança jurídica para o setor público e privado.

**II. OBJETIVOS ESPECÍFICOS:**

1. Identificar desafios regulatórios e práticos relacionados ao tratamento de dados pessoais nas relações de trabalho.
2. Identificar e analisar práticas corporativas envolvendo o tratamento de dados pessoais de empregados, terceiros e candidatos.
3. Realizar estudos técnicos sobre temas críticos.
4. Propor recomendações para orientar agentes de tratamento e titulares de dados no ambiente laboral.

**III. METODOLOGIA DE TRABALHO:**

1. **Revisão Doutrinária e Jurisprudencial:** Análise de literatura nacional e internacional, bem como de decisões judiciais e administrativas relevantes.
2. **Análise de Boas Práticas:** Diagnóstico comparado com boas práticas nacionais e internacionais.
3. **Consulta a Especialistas:** Convocação de especialistas, sociedade civil, sindicatos, associações empresariais, academia e outros atores relevantes para contribuir com os trabalhos.
4. **Discussões Colaborativas:** Reuniões ordinárias para debate e deliberação sobre os temas em pauta.

#### IV. CRONOGRAMA DE ATIVIDADES (120 DIAS):

<b>Etapa</b>	<b>Atividade Principal</b>	<b>Entregas Parciais</b>	<b>Período (Dias Corridos)</b>
<b>1</b>	<b>Organização e Planejamento Detalhado</b>	- Estruturação inicial e divisão de tarefas. - Cronograma executivo e de reuniões.	1-15
<b>2</b>	<b>Mapeamento de Temas e Revisão Inicial</b>	- Documento com o mapeamento dos eixos temáticos prioritários. - Relatório preliminar de revisão bibliográfica.	16-45
<b>3</b>	<b>Análise Aprofundada e Audiências</b>	- Realização de ciclos de discussão com especialistas. - Minutas iniciais de tópicos do relatório.	46-90
<b>4</b>	<b>Consolidação e Redação do Relatório Final</b>	- Versão consolidada do relatório para apreciação interna do GT. - Relatório Final assinado e submetido ao CNPD.	91-120

## V. PRODUTOS/ENTREGAS:

O produto do Grupo de Trabalho será um **Relatório final** contendo, no mínimo:

1. **Histórico das Atividades:** Descrição detalhada de todas as atividades realizadas pelo GT.
2. **Produtos Elaborados:** Podendo incluir:
  - a. Estudos técnicos sobre temas específicos
  - b. Diretrizes ou Recomendações para agentes de tratamento.
3. **Parecer Conclusivo:** Síntese dos achados e proposições finais para subsidiar a atuação da ANPD na temática laboral.

## VI. CRONOGRAMA DE REUNIÕES:

- **Periodicidade:** Semanal / Quinzenal (a definir pelo GT)
- **Datas:** (a definir pelo GT)
- **Formato:** Videoconferência.

## VII. DIVULGAÇÃO DE ATIVIDADES E PRESTAÇÃO DE CONTAS:

- O andamento dos trabalhos será regularmente informado pela Coordenação do GT nas reuniões do CNPD, conforme determina a Portaria.

## Anexo 3 – Atas das reuniões realizadas



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA  
PRIVACIDADE (CNPd)  
GRUPO DE TRABALHO 1 - PROTEÇÃO DE DADOS NO CONTEXTO LABORAL  
ATA DA 1ª REUNIÃO ORDINÁRIA**

**Data:** 24/11/2025

**Hora de Início:** 16:00

**Hora de Término:** 17:00

**Modalidade:** Videoconferência.

**I. MEMBROS PRESENTES:**

- Débora Sirotheau Siqueira Rodrigues (Coordenadora e Relatora)
- Alexandre Zago Boava;
- Cassio Augusto Muniz Borges;
- João Marcos Pereira Vidal

**II. MEMBROS AUSENTES/JUSTIFICADAS:**

- Isabella Vieira Machado Henriques.
- Gabrielle Bezerra Sales Sarlet (saiu do grupo)

**III. CONVIDADOS/ESPECIALISTAS:**

- Não aplicável nesta reunião.

**IV. PAUTA:**

1. Aprovação do Plano de Trabalho.
2. Definição do Calendário de reuniões.
3. Definição do Coordenador(a) Suplente.
4. Definição dos convidados por eixo temático.

**V. DELIBERAÇÕES E ENCAMINHAMENTOS:**

Item	Deliberação/Encaminhamento	Responsável	Prazo
------	----------------------------	-------------	-------

1	O Plano de Trabalho foi aprovado.	-	-
2	Os encontros serão semanais e ocorrerão toda segunda-feira, as 16:00.	-	-
3	O suplente será Alexandre Zago Boava.	-	-
4	Foi apresentado uma proposta de eixos temáticos.		
5	Próxima reunião: analisar os eixos temáticos e os nomes dos especialistas.	-	-

#### **VI. INFORMAÇÕES GERAIS (INFORMES):**

- A Coordenadora explicou o modelo de plano de trabalho proposto e aprovado por todos.
- O suplente foi escolhido com aprovação de todos.
- Gabrielle Bezerra Sales Sarlet teve de deixar o grupo de trabalho, com isso o seu nome será retirado das próximas atas.

#### **VII. PRÓXIMA REUNIÃO:**

**Data:** 01/12/2025

**Hora:** 16:00

**Pauta Preliminar:**

- Análise dos eixos temáticos;
- Indicação dos especialistas.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT1 - Proteção de Dados no Contexto Laboral  
CNPd



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA  
PRIVACIDADE (CNPd)  
GRUPO DE TRABALHO 1 - PROTEÇÃO DE DADOS NO CONTEXTO LABORAL  
ATA DA 2ª REUNIÃO ORDINÁRIA**

**Data:** 01/12/2025

**Hora de Início:** 16:00

**Hora de Término:** 17:00

**Modalidade:** Videoconferência.

**I. MEMBROS PRESENTES:**

- Débora Sirotheau Siqueira Rodrigues (Coordenadora e Relatora)
- Alexandre Zago Boava;
- Cassio Augusto Muniz Borges;
- Isabella Vieira Machado Henriques.

**II. MEMBROS AUSENTES/JUSTIFICADAS:**

- João Marcos Pereira Vidal.

**III. CONVIDADOS/ESPECIALISTAS:**

- Não aplicável nesta reunião.

**IV. PAUTA:**

1. Análise e ajustes nos eixos temáticos;
2. Estratégia de definição de convidados para os eixos temáticos.

**V. DELIBERAÇÕES E ENCAMINHAMENTOS:**

Item	Deliberação/Encaminhamento	Responsável	Prazo
1	Ata da reunião anterior homologada por todos.	-	-

2	Ajustes realizados nos eixos temáticos, com o propósito de reduzir o escopo e ajustes nos textos das perguntas de cada eixo.	-	-
3	Próxima reunião: - Analisar outros especialistas, de outras entidades. - Analisar perguntas dos eixos temáticos.	-	-

## VI. INFORMAÇÕES GERAIS (INFORMES):

- Após os ajustes realizados nos eixos temáticos o grupo entendeu que a melhor estratégia seria convidar, primeiro, os especialistas integrantes da ANPD e, depois, os especialistas de outras instituições.
- Os convites serão enviados, de acordo com os eixos temáticos.

## VII. PRÓXIMA REUNIÃO:

**Data:** 08/12/2025

**Hora:** 16:00

**Pauta Preliminar:**

- Nova análise das perguntas dos eixos temáticos.
- Outros especialistas, de outras entidades, para serem convidados.

**Débora Sirotheau Siqueira Rodrigues**

Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPD



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA  
PRIVACIDADE (CNPD)**

## GRUPO DE TRABALHO 1 - PROTEÇÃO DE DADOS NO CONTEXTO LABORAL

### ATA DA 3ª REUNIÃO ORDINÁRIA

**Data:** 08/12/2025

**Hora de Início:** 16:00

**Hora de Término:** 17:00

**Modalidade:** Videoconferência.

#### **I. MEMBROS PRESENTES:**

- Débora Sirotheau Siqueira Rodrigues (Coordenadora e Relatora)
- Alexandre Zago Boava;
- Cassio Augusto Muniz Borges;
- Isabella Vieira Machado Henriques.

#### **II. MEMBROS AUSENTES/JUSTIFICADAS:**

- João Marcos Pereira Vidal.

#### **III. CONVIDADOS/ESPECIALISTAS:**

- Não aplicável nesta reunião.

#### **IV. PAUTA:**

1. Análise e ajustes das perguntas do eixo temático;
2. Outros especialistas, de outras entidades, para serem convidados.

#### **V. DELIBERAÇÕES E ENCAMINHAMENTOS:**

Item	Deliberação/Encaminhamento	Responsável	Prazo
1	Ata da reunião anterior homologada por todos.	-	-
2	Todas as perguntas contidas dos eixos temáticos foram lidas, discutidas e homologadas com os participantes, sendo enviada a última versão.	-	-
3	As discussões sobre os especialistas ficaram focadas no âmbito da ANPD.	-	-

4

Próxima reunião:

- Tentar levantar os acordos coletivos que tem temas de proteção de dados, avisos de privacidades para trabalhadores e relação de especialistas.

## **VI. INFORMAÇÕES GERAIS (INFORMES):**

- Foi manifestado preocupação com a complexidade das perguntas, pois algumas delas demandaria estudo com tempo de duração maior que o tempo de duração do próprio GT1.
- Foi observado a dificuldade de agenda, em função do período de final de ano (festividades, fechamento de ano, férias, etc), o que pode impactar o andamento do GT1.

## **VII. PRÓXIMA REUNIÃO:**

**Data:** 15/12/2025

**Hora:** 16:00

**Pauta Preliminar:**

- Acordos coletivos que tem temas de proteção de dados, avisos de privacidades para trabalhadores;
- Avisos de privacidades para trabalhadores;
- Relação de especialistas.

**Débora Sirotheau Siqueira Rodrigues**

Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd



**CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA  
PRIVACIDADE (CNPd)  
GRUPO DE TRABALHO 1 - PROTEÇÃO DE DADOS NO CONTEXTO LABORAL  
ATA DA 4ª REUNIÃO ORDINÁRIA**

**Data:** 05/01/2026

**Hora de Início:** 16:00

**Hora de Término:** 17:00

**Modalidade:** Videoconferência.

**I. MEMBROS PRESENTES:**

- Débora Sirotheau Siqueira Rodrigues (Coordenadora e Relatora)
- Alexandre Zago Boava;
- Cassio Augusto Muniz Borges;
- Isabella Vieira Machado Henriques.

**II. MEMBROS AUSENTES/JUSTIFICADAS:**

- João Marcos Pereira Vidal.

**III. CONVIDADOS/MJSP:**

- Kamilla Mariana Martins Rodrigues - MJSP

**IV. PAUTA:**

1. Reorganização e retomada das tarefas, após período festivo de final de ano;
2. Distribuição dos membros por eixos temáticos;
3. Definição dos próximos especialistas e instituições a serem convidadas.

**V. DELIBERAÇÕES E ENCAMINHAMENTOS:**

Item	Deliberação/Encaminhamento	Responsável	Prazo
1	Ata da reunião anterior homologada por todos.	-	-
2	<p>Débora informou que:</p> <ul style="list-style-type: none"> <li>- Já pediu apoio à CUT na parte de acordo coletivo.</li> <li>- Formalizará pedido de apoio junto ao INPD, SERPRO e Dataprivacy Brasil.</li> <li>- Formalizará pedido de apoio também para as professoras Caroline (acordo coletivo) e Selma (bases legais), bem como a empresa de DPO as a Service desta última.</li> </ul>	-	-

3	Isabella sugeriu abordar a questão de benefícios de trabalhadores que envolvem crianças e adolescentes e o trabalho de menor aprendiz, abrangendo princípios e bases legais. Ela informou que já possui alguns materiais e enviará algo bem sucinto.	-	-
4	Cassio encaminhará os canais de comunicação das instituições selecionadas para participarem e sugeriu que fosse ressaltado a citação de casos práticos, pelas entidades convidadas.	-	-
5	<p>Foi proposto a alocação dos membros conforme os eixos do trabalho e ficou assim distribuído:</p> <p>Alexandre - Monitoramento</p> <p>Isabella - Dados de Crianças e Adolescentes e Benefícios</p> <p>João Vidal - Diálogo social</p> <p>Debora - Transparência e direitos dos titulares</p> <p>Cassio - Princípios e bases legais</p>		

## **VI. INFORMACÕES GERAIS (INFORMES):**

- Novamente foi manifestado preocupação com a complexidade das perguntas, pois algumas delas demandaria estudo com tempo de duração maior que o tempo de duração do próprio GT1.

## **VII. PRÓXIMA REUNIÃO:**

**Data:** 12/01/2026

**Hora:** 16:00

**Pauta Preliminar:**

- Continuidade dos trabalhos já definidos.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

## Anexo 4 – Registro das entrevistas com especialistas e entidades

### ATA DE ENTREVISTA

**Data:** 17/12/2025

**Horário:** 19:00 as 20:51

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Cassio Augusto Muniz Borges, Kamilla Mariana Martins Rodrigues, Albert Franca Josua Costa (Substituto da Coordenação-Geral de Tecnologia e Pesquisa - CGTP), Rodrigo Santana dos Santos (Coordenador-Geral de Normas - CGN) e Jorge Andre Ferreira Fontelles de Lima (Coordenador de Fiscalização, substituto)

ENTREVISTADA: ANPD

**Agência Nacional de Proteção de Dados**

**As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.**

**Sumário executivo da visão da entrevistada:**

**1) Apresentação Inicial:** Débora Sirotheau apresentou o GT1, seus membros e o objetivo de desenvolver um trabalho que agregue valor prático à ANPD, ouvindo as necessidades das coordenações envolvidas (Fiscalização, Normatização e Pesquisa).

#### **2) Contribuições das Coordenações da ANPD:**

- **CGTP (Pesquisa – Albert):** Foram destacados dois eixos prioritários para pesquisa:
  - **Ferramentas de IA no RH:** Riscos de viés discriminatório e opacidade em algoritmos usados para recrutamento, seleção e gestão de pessoas.
  - **Ferramentas de monitoramento:** Especialmente as baseadas em geolocalização, com riscos à privacidade, inferência indevida sobre estado de saúde ou filiação sindical, e uso secundário dos dados.
- **CGN (Normatização – Rodrigo):** Foram apontadas lacunas e desafios regulatórios a serem explorados:
  - Aplicação de bases legais (execução de contrato, legítimo interesse) no contexto laboral.
  - Transparência e canais de atendimento ao titular (trabalhador) - adequação de avisos de privacidade e mecanismos internos.
  - Uso de tecnologias como reconhecimento facial para controle de acesso/ponto e monitoramento por câmeras ou geolocalização.
  - Ações educativas voltadas aos trabalhadores.
- **Fiscalização (Jorge):** A perspectiva foi de que o tema deve ganhar prioridade no próximo biênio, focando na **proteção dos direitos dos titulares (trabalhadores)**. Preocupações específicas:

- **Fase pré-contratual:** Decisões automatizadas e vieses em plataformas de recrutamento.
- **Fase contratual:** Vigilância excessiva, coleta de dados além do necessário e uso secundário (ex.: dados usados para treinar IA sem aviso).

### 3) Debate sobre Escopo e Formato do Trabalho do GT1:

- Foi consenso que o tema é vasto e o tempo do GT é curto, exigindo priorização.
- Sugeriu-se um trabalho em duas fases: 1) abordagem de aspectos basilares (princípios, bases legais, transparência); 2) tópicos mais complexos (monitoramento).
- Quanto ao formato da entrega, discutiu-se a criação de um **relatório**, preferencialmente baseado na identificação de **problemas concretos** e **estudos de caso** (hipotéticos ou anonimizados, inspirados em situações reais) para ilustrar e direcionar as orientações.
- Foi destacada a importância de ter uma linguagem prática, possivelmente seguindo o fluxo do processo laboral (pré-contrato, durante e pós-contrato).

### 4) Encaminhamentos e Combinados:

- O GT1 irá priorizar os pontos levantados, com foco inicial nos itens considerados mais basilares e urgentes.
- Haverá **nova reunião de alinhamento** no decorrer dos trabalhos para validação do rumo e dos estudos de caso desenvolvidos pelo GT, assegurando a utilidade prática do material para a ANPD.
- Serão buscados subsídios com especialistas e DPOs atuantes na área laboral para embasar os estudos de caso.

### 5) Conclusão

A reunião foi considerada muito produtiva pelas partes, estabelecendo um canal aberto de diálogo e um direcionamento claro para os trabalhos do GT1. Ficou evidenciada a relevância do tema para a ANPD e a expectativa de que o GT produza subsídios práticos e focados em problemas reais.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPD

Horário: 16:00 as 17:20

Participantes: Débora Sirotheau Siqueira Rodrigues, Alexandre Zago, Cassio Augusto, Kamila Mariana.

---

**ENTREVISTADA: CAROLINE DE MELO LIMA GULARTE**

Mentora de empresas, escritórios de advocacia e advogados que escalam negócios com Compliance Trabalhista, Governança em IA e Proteção de Dados | Advogada e Consultora Jurídica Trabalhista | Professora | CEO @c4data

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

## 1. Finalidades e bases legais no contexto laboral

O material evidencia um problema estrutural recorrente que se verifica na prática de quem atua com proteção de dados pessoais nas relações de trabalho: a formulação de finalidades amplas, genéricas ou elásticas no tratamento de dados de trabalhadores, como “gestão de pessoas” ou “interesse empresarial”, que não atendem ao princípio da finalidade (art. 6º, inc. I da LGPD). Essas formulações:

- não oferecem previsibilidade ao titular,
- inviabilizam a avaliação de necessidade,
- ampliam indevidamente o escopo do tratamento.

### Como resposta técnica, propõe-se:

- fragmentação das finalidades por fase da relação laboral (recrutamento, contrato e pós-contrato de trabalho);
- vinculação de cada finalidade a uma base legal específica;
- redação operacional e verificável, e não abstrata (ex.: controle de jornada para cumprimento do art. 74 da CLT).

Quanto às bases legais, o material reforça que o consentimento é, como regra, inadequado no vínculo empregatício, em razão do desequilíbrio estrutural de poder — posição alinhada à legislação e às autoridades de proteção de dados internacionais. O uso do legítimo interesse exige teste tripartite documentado, consideração das expectativas legítimas do trabalhador e salvaguardas adicionais, como RIPD e revisão periódica.

O uso abusivo de “obrigação legal” como base genérica também é criticado, exigindo sempre indicação da norma específica, delimitação temporal e cessação do tratamento ao fim da obrigação.

## 2. Princípio da necessidade e práticas excessivas

Os documentos demonstram que a coleta excessiva de dados no trabalho é sistêmica, impulsionada por soluções tecnológicas prontas, cultura de acumulação e insegurança jurídica.

O princípio da necessidade (art. 6º, inc. III da LGPD) é tratado como avaliação qualitativa, exigindo análise de:

- indispensabilidade do dado;
- existência de meios menos invasivos;
- possibilidade de anonimização, pseudonimização, agregação.

#### **São apontadas como práticas críticas:**

- recrutamento e seleção de candidatos (coleta excessiva de dados pessoais em redes sociais, testes que avaliam a saúde mental de trabalhadores, sem qualquer relação com o trabalho, uso de inteligência artificial, revelando tratamento de dados pessoais de alto risco, potencializando discriminação na fase pré contratual);
- biometria, sem avaliação de alternativas menos invasivas (com referência à Resolução ANPD nº 23/2025);
- monitoramento digital intrusivo (captura de tela, digitação, webcam), especialmente para trabalhadores em regime de teletrabalho;
- people analytics sem RIPD.

Caroline destaca precedente do TRT da 15ª Região, em ACP envolvendo plataformas de recrutamento, com condenação por dano moral coletivo e imposição de obrigações de governança (DPO, ROPA, transparência e minimização), reforçando a centralidade da LGPD no meio ambiente do trabalho digital.

### **3. Transparência, direitos dos trabalhadores e decisões automatizadas**

A transparência é tratada como condição de legitimidade, não como formalidade. Observa-se que:

- avisos de privacidade específicos para o contexto laboral ainda são raros;
- prevalecem documentos genéricos e pouco acessíveis.

#### **Boas práticas indicadas:**

- avisos segmentados por fase da relação laboral;
- linguagem clara e não jurídica;
- atualização contínua. Há ênfase no crescimento do uso secundário de dados (treinamento de IA, automação decisória, analytics preditivo), alertando que, sem base legal específica, configura desvio de finalidade. Em decisões automatizadas, destaca-se a baixa efetividade prática do art. 20 da LGPD, diante da ausência de revisão humana, instâncias recursais e canais acessíveis de contestação — tema aprofundado no caso de bloqueios de entregadores por plataformas.

### **4. Monitoramento, produtividade e riscos discriminatórios**

O monitoramento laboral é tratado como atividade de alto risco, exigindo:

- avaliação prévia de impacto;
- limitação temporal;
- vedação de vigilância contínua;
- transparência reforçada;
- auditoria algorítmica e governança clara. São destacados os riscos discriminatórios decorrentes de vieses históricos, métricas enviesadas e penalizações indiretas, agravados pela ausência de RIPD. O material dialoga com experiências internacionais, que reforçam a necessidade de proporcionalidade, intervenção mínima e participação dos trabalhadores na definição dessas práticas.

## **5. Diálogo social, negociação coletiva e direito comparado**

Um eixo central do material é a articulação entre proteção de dados e negociação coletiva, especialmente após a Reforma Trabalhista (arts. 611-A, 611-B e 620 da CLT). Apesar do potencial normativo, o diagnóstico é de cláusulas ainda incipientes e pouco técnicas no Brasil.

### **O direito comparado demonstra caminhos mais maduros:**

- Espanha: positividade expressa dos direitos digitais trabalhistas (intimidade, desconexão, geolocalização, videovigilância) e participação sindical.
- Alemanha: legitimação do tratamento de dados laborais por meio de convenções coletivas, inclusive dados sensíveis, com salvaguardas.
- Argentina e Chile: exigência de participação sindical e incorporação das regras de proteção de dados aos contratos e regulamentos internos.
- Califórnia (CCPA): vedação expressa à retaliação contra empregados ou candidatos que exerçam direitos de proteção de dados.
- China (PIPL): classificação rigorosa de dados sensíveis e obrigatoriedade de DPIA, com forte enfoque em segurança e governança

## **6. Síntese estratégica**

A proteção de dados no ambiente de trabalho não é um apêndice da LGPD, mas um eixo estruturante do meio ambiente laboral digital. A ausência de finalidades claras, de bases legais bem delimitadas, de RIPD e de diálogo social também expõe empregadores a riscos jurídicos, regulatórios, reputacionais e discriminatórios, especialmente diante da expansão de IA, monitoramento e automação decisória.

### **Caroline sustenta, de forma consistente, a necessidade de:**

- accountability demonstrável;
- integração entre compliance trabalhista, governança de IA e proteção de dados nas relações laborais;

- o fortalecimento da negociação coletiva para discussão dos novos temas que afetam o ambiente de trabalho;
- uso estratégico do direito comparado para preencher lacunas normativas no Brasil, conforme o art. 8º da CLT.

**Fim dos registros.**

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

## ATA DE ENTREVISTA

**Data:** 16/01/2026

**Horário:** 16:00 as 17:30

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Cassio Augusto Muniz Borges, Rodrigo Santana dos Santos (CGN), Jorge Andre Ferreira Fontelles de Lima (Coord. de Fiscalização, substituto), Albert Franca Josua Costa (Tecnologia e Pesquisa, substituto), Kamilla Mariana Martins Rodrigues

---

ENTREVISTADA: ANPD

**Agência Nacional de Proteção de Dados**

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

### 1. EXPOSIÇÃO DAS COORDENAÇÕES DA ANPD

- **Coordenação de Tecnologia e Pesquisa (CGTP) – Albert Costa:**

**Riscos Emergentes Priorizados:**

- **Ferramentas de IA para Gestão de Pessoas:** Utilizadas em recrutamento, seleção e avaliação de desempenho. Riscos: vieses discriminatórios e opacidade das decisões automatizadas.
- **Ferramentas de Monitoramento do Trabalho:** Especialmente as que utilizam geolocalização (ex.: aplicativo TIMS). Riscos: violação da privacidade (inclusive fora do horário de serviço), inferência indevida sobre estado de saúde ou posições políticas/sindicais, e uso secundário dos dados fora da finalidade original.

- **Coordenação de Governança Normativa (CGN) – Rodrigo Santos:**

**Lacunas e Desafios Regulatórios Identificados:**

- **Hipóteses Legais:** Necessidade de aprofundar o uso da **execução de contrato** e do **legítimo interesse** no contexto laboral.

- **Finalidade e Compatibilidade:** Definir parâmetros para avaliar a compatibilidade de finalidades, especialmente em tratamentos secundários ou compartilhamentos.
  - **Transparência e Comunicação:** Adaptar instrumentos como o **aviso de privacidade** e os **canais de atendimento** para o público interno (trabalhadores).
  - **Tecnologias Intrusivas:** Regulação do uso de **reconhecimento facial** (ex.: para bater ponto) e **geolocalização**, balanceando os interesses da empresa e o direito à privacidade.
  - **Decisões Automatizadas e Não-Discriminação:** Combate a vieses em algoritmos de seleção.
  - **Ações Educativas:** Desenvolver ações específicas para capacitar trabalhadores sobre seus direitos na LGPD.
- **Coordenação de Fiscalização – Jorge Fontelles:**
    - **Foco da Atuação Futura (Próximo Biênio):** A fiscalização provavelmente terá como tema prioritário a "**Proteção de Direitos dos Titulares**", com enfoque no contexto laboral.
    - o **Preocupações Específicas:**
      - **Fase Pré-Contratual:** Decisões automatizadas em plataformas de recrutamento e riscos de vieses discriminatórios.
      - **Fase Contratual:** Vigilância excessiva, coleta de dados além do necessário (ex.: softwares de produtividade em home office) e **uso secundário de dados** (ex.: para treinamento de modelos de IA sem base legal ou transparência).
- Autoaplicabilidade da LGPD:** Ressaltou que as normas da LGPD já são aplicáveis ao mercado de trabalho, permitindo ação fiscalizatória mesmo sem regulamentação setorial específica, atuando de forma proporcional e priorizando medidas preventivas em casos de dúvida razoável.

## 2. DEBATE E DEFINIÇÃO DE METODOLOGIA DE TRABALHO

- **Consenso sobre a Abordagem:** Ficou claro que o tema é **relevante e prioritário** para a ANPD, embora não esteja na agenda imediata do biênio em curso.
- **Temas Prioritários Mencionados para o Guia:** Minimização de dados, finalidade, transparência (avisos de privacidade), bases legais (com foco nos equívocos no uso do consentimento), direitos dos titulares e o papel da **negociação coletiva** como instrumento complementar de regulamentação setorial.

**Encerramento:** A reunião foi encerrada de forma colaborativa, com os representantes da ANPD se colocando à disposição para o debate contínuo e parabenizando a iniciativa do GT1.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

## ATA DE ENTREVISTA

**Data:** 19/01/2026

**Horário:** 16:00 as 17:30

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Alexandre Boava, Renan Bernardi Kalil, Cassio Augusto Muniz Borges, Kamila Mariana Martins Rodrigues, Roseli Figaro.

---

**ENTREVISTADA: RENAN BERNARDI KALIL**

**Procurador do Trabalho no Ministério Público do Trabalho | Professor de Direito no Insper.**

---

**As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.**

**Sumário executivo da visão da entrevistada:**

### **1. EXPOSIÇÃO INICIAL – DR. RENAN BERNARDI KALIL**

- **Contexto:** Dr. Renan atuou na Coordenadoria Nacional de Combate às Fraudes Trabalhistas do MPT e trouxe uma perspectiva focada em trabalhadores de plataformas digitais (motoristas e entregadores), independentemente da discussão sobre a natureza jurídica do vínculo.
- **Problemas Identificados:**
  - Gestão Algorítmica Opaca:** As plataformas utilizam algoritmos para gerenciar o trabalho (direcionamento de demandas, promoções, bloqueios) de forma automatizada e sem transparência para o trabalhador.
  - Descumprimento do Art. 20 da LGPD:** Bloqueios e suspensões de contas ocorrem de forma automatizada, com notificações genéricas, violando o direito do titular à revisão e explicação sobre decisões que afetam seus interesses profissionais.
  - Exemplos de Impacto:** Citou casos concretos envolvendo a plataforma "iaudite" (erros em checagem de antecedentes) e o iFood (racismo algorítmico em reconhecimento facial), que resultaram em bloqueios injustos e na necessidade de judicialização para reversão.

**Dificuldade de Acesso a Dados:** Compartilhou a experiência do MPT em obter dados das plataformas, destacando a resistência das empresas mesmo perante requisições oficiais.

- **Sugestões e Encaminhamentos:**

**Efetivação do Art. 20:** É urgente garantir o direito à explicação e revisão de decisões automatizadas para trabalhadores.

**Papel da ANPD:** Sugeriu que a Agência utilize suas atribuições (art. 55 da LGPD) para regulamentar e promover a transparência no tratamento de dados dos trabalhadores, especialmente em processos de revisão.

**Referência Jurídica:** Citou decisão da Ministra Nancy Andrighi (STJ/2023) que reconhece a aplicação do art. 20 da LGPD a bloqueios automatizados em plataformas.

## 2. EXPOSIÇÃO – PROF.<sup>a</sup> ROSELI FIGARO

- **Contexto Macro:** Apresentou uma análise estrutural da economia digital, introduzindo o conceito de uma **nova cadeia produtiva digital de dados**, liderada por grandes empresas transnacionais que controlam a infraestrutura tecnológica (nuvem, software).

- **Problemas Estruturais Identificados:**

**Hegemonia e Dependência:** As demais cadeias produtivas (agronegócio, indústria, serviços) tornam-se dependentes dessa infraestrutura estrangeira, cedendo o controle sobre seus dados e, por consequência, sobre aspectos de sua operação e soberania.

**Datificação do Trabalho:** O gerenciamento algorítmico é a evolução em tempo real da gestão científica do trabalho (taylorismo/toyotismo), tendo como matéria-prima os dados dos trabalhadores para aumentar produtividade e gerar novos produtos/patentes.

**Falta de Regulação Efetiva:** Os verdadeiros "reguladores" atuais são os Termos de Uso das grandes plataformas, que operam sem contrapesos nacionais efetivos.

**Impacto Ampliado:** A questão dos dados laborais está intrinsecamente ligada a problemas maiores como soberania nacional, geopolítica dos recursos (terras raras) e o modelo de desenvolvimento do país.

- **Sugestões e Encaminhamentos:**

**Visão Sistêmica:** A LGPD e a atuação da ANPD devem ser vistas como instrumentos estratégicos para um projeto nacional de soberania e desenvolvimento, não apenas como regulação pontual.

**Ação Estruturante:** É necessário pensar a regulação do trabalho e dos dados de forma articulada com a construção de infraestrutura tecnológica nacional e a valorização do conhecimento científico brasileiro.

## 3. DEBATE E CONSIDERAÇÕES FINAIS

- **Alexandre Boava** problematizou o argumento das plataformas sobre a "inviabilidade" de revisões humanas (como apresentado em documento da MobTech), questionando se

o modelo de negócio atual não se baseia na não-aplicação de direitos. Destacou a LGPD também como ferramenta de proteção e soberania para empresas nacionais.

- **Debora Sirotheau** reforçou a necessidade de equilíbrio entre inovação e garantia de direitos fundamentais. Solicitou a identificação de **boas práticas** (ex.: mediação pré-processual) que possam servir de modelo, e a facilitação de diálogo com a coordenação atual do MPT para aprofundar casos concretos.
- **Dr. Renan** rebateu o argumento da "inviabilidade", caracterizando-o como uma estratégia recorrente das plataformas para evitar qualquer regulação. Ressaltou que o Brasil é um mercado crucial para essas empresas globais e que os patamares de proteção estabelecidos aqui são relevantes no cenário internacional.
- Foi consenso que a **figura do trabalhador como titular de dados** deve ser plenamente reconhecida, garantindo-lhe todos os direitos da LGPD, para além de uma mera condição de parte em "execução de contrato".

#### ENCAMINHAMENTOS PROPOSTOS:

1. **Aprofundar a discussão sobre a efetivação do Art. 20 da LGPD** no contexto laboral, com foco em transparência e revisão de decisões automatizadas.
2. **Explorar o papel regulatório da ANPD** (com base no Art. 55) para editar normas e promover a proteção de dados dos trabalhadores.
3. **Identificar e analisar boas práticas** (mesmo que incipientes) adotadas por plataformas para enfrentar os problemas discutidos.
4. **Estabelecer interlocução** com a Coordenadoria Nacional de Combate às Fraudes Trabalhistas do MPT para troca de informações e casos.
5. **Manter a perspectiva macro** da regulação de dados como elemento de soberania nacional e desenvolvimento de infraestrutura tecnológica brasileira.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

#### ATA DE ENTREVISTA

**Data:** 19/01/2026

**Horário:** 16:00 as 17:30

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Alexandre Boava, Renan Bernardi Kalil, Cassio Augusto Muniz Borges, Kamila Mariana Martins Rodrigues, Roseli Figaro.

---

ENTREVISTADA: ROSELI APARECIDA FIGARO PAULINO

Professora titular da Universidade de São Paulo | Bolsista Produtividade em Pesquisa do CNPq, Nível 2 |  
Coordenadora do Centro de Pesquisa em Comunicação e Trabalho (CPCT)

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

## 1. EXPOSIÇÃO INICIAL – DR. RENAN BERNARDI KALIL

- **Contexto:** Dr. Renan atuou na Coordenadoria Nacional de Combate às Fraudes Trabalhistas do MPT e trouxe uma perspectiva focada em trabalhadores de plataformas digitais (motoristas e entregadores), independentemente da discussão sobre a natureza jurídica do vínculo.
- **Problemas Identificados:**
  - Gestão Algorítmica Opaca:** As plataformas utilizam algoritmos para gerenciar o trabalho (direcionamento de demandas, promoções, bloqueios) de forma automatizada e sem transparência para o trabalhador.
  - Descumprimento do Art. 20 da LGPD:** Bloqueios e suspensões de contas ocorrem de forma automatizada, com notificações genéricas, violando o direito do titular à revisão e explicação sobre decisões que afetam seus interesses profissionais.
  - Exemplos de Impacto:** Citou casos concretos envolvendo a plataforma "iaudite" (erros em checagem de antecedentes) e o iFood (racismo algorítmico em reconhecimento facial), que resultaram em bloqueios injustos e na necessidade de judicialização para reversão.
  - Dificuldade de Acesso a Dados:** Compartilhou a experiência do MPT em obter dados das plataformas, destacando a resistência das empresas mesmo perante requisições oficiais.
- **Sugestões e Encaminhamentos:**
  - Efetivação do Art. 20:** É urgente garantir o direito à explicação e revisão de decisões automatizadas para trabalhadores.
  - Papel da ANPD:** Sugeriu que a Agência utilize suas atribuições (art. 55 da LGPD) para regulamentar e promover a transparência no tratamento de dados dos trabalhadores, especialmente em processos de revisão.
  - Referência Jurídica:** Citou decisão da Ministra Nancy Andrighi (STJ/2023) que reconhece a aplicação do art. 20 da LGPD a bloqueios automatizados em plataformas.

## 2. EXPOSIÇÃO – PROF.<sup>a</sup> ROSELI FIGARO

- **Contexto Macro:** Apresentou uma análise estrutural da economia digital, introduzindo o conceito de uma **nova cadeia produtiva digital de dados**, liderada por grandes empresas transnacionais que controlam a infraestrutura tecnológica (nuvem, software).

**Problemas Estruturais Identificados:**

**Hegemonia e Dependência:** As demais cadeias produtivas (agronegócio, indústria, serviços) tornam-se dependentes dessa infraestrutura estrangeira, cedendo o controle sobre seus dados e, por consequência, sobre aspectos de sua operação e soberania.

**Datificação do Trabalho:** O gerenciamento algorítmico é a evolução em tempo real da gestão científica do trabalho (taylorismo/toyotismo), tendo como matéria-prima os dados dos trabalhadores para aumentar produtividade e gerar novos produtos/patentes.

**Falta de Regulação Efetiva:** Os verdadeiros "reguladores" atuais são os Termos de Uso das grandes plataformas, que operam sem contrapesos nacionais efetivos.

**Impacto Ampliado:** A questão dos dados laborais está intrinsecamente ligada a problemas maiores como soberania nacional, geopolítica dos recursos (terras raras) e o modelo de desenvolvimento do país.

- **Sugestões e Encaminhamentos:**

**Visão Sistêmica:** A LGPD e a atuação da ANPD devem ser vistas como instrumentos estratégicos para um projeto nacional de soberania e desenvolvimento, não apenas como regulação pontual.

**Ação Estruturante:** É necessário pensar a regulação do trabalho e dos dados de forma articulada com a construção de infraestrutura tecnológica nacional e a valorização do conhecimento científico brasileiro.

### 3. DEBATE E CONSIDERAÇÕES FINAIS

- **Alexandre Boava** problematizou o argumento das plataformas sobre a "inviabilidade" de revisões humanas (como apresentado em documento da MobTech), questionando se o modelo de negócio atual não se baseia na não-aplicação de direitos. Destacou a LGPD também como ferramenta de proteção e soberania para empresas nacionais.
- **Debora Sirotheau** reforçou a necessidade de equilíbrio entre inovação e garantia de direitos fundamentais. Solicitou a identificação de **boas práticas** (ex.: mediação pré-processual) que possam servir de modelo, e a facilitação de diálogo com a coordenação atual do MPT para aprofundar casos concretos.
- **Dr. Renan** rebateu o argumento da "inviabilidade", caracterizando-o como uma estratégia recorrente das plataformas para evitar qualquer regulação. Ressaltou que o Brasil é um mercado crucial para essas empresas globais e que os patamares de proteção estabelecidos aqui são relevantes no cenário internacional.
- Foi consenso que a **figura do trabalhador como titular de dados** deve ser plenamente reconhecida, garantindo-lhe todos os direitos da LGPD, para além de uma mera condição de parte em "execução de contrato".

### ENCAMINHAMENTOS PROPOSTOS:

1. **Aprofundar a discussão sobre a efetivação do Art. 20 da LGPD** no contexto laboral, com foco em transparência e revisão de decisões automatizadas.
2. **Explorar o papel regulatório da ANPD** (com base no Art. 55) para editar normas e promover a proteção de dados dos trabalhadores.
3. **Identificar e analisar boas práticas** (mesmo que incipientes) adotadas por plataformas para enfrentar os problemas discutidos.

4. **Estabelecer interlocução** com a Coordenadoria Nacional de Combate às Fraudes Trabalhistas do MPT para troca de informações e casos.
5. **Manter a perspectiva macro** da regulação de dados como elemento de soberania nacional e desenvolvimento de infraestrutura tecnológica brasileira.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPD

## ATA DE ENTREVISTA

**Data:** 26/01/2026

**Horário:** 16:00 as 17:30

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Alexandre Boava, Cassio Augusto, Volia Bomfim, Carolina Tupinambá, Kamila Mariana Martins, Isabella Henriques

---

**ENTREVISTADAS: VOLIA BONFIM e CAROLINA TUPINAMBÁ**

**Volia: Advogada Trabalhista, e**  
**Carolina: Advogada e Professora**

---

**As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.**

**Sumário executivo da visão da entrevistada:**

### 1. EXPOSIÇÃO – DRA. CAROLINA TUPINAMBÁ

**Tema Central:** A aplicação da LGPD em contextos de trabalho com e sem vínculo de subordinação e os limites do monitoramento e vigilância.

- **Premissa Fundamental:** A LGPD se aplica plenamente tanto às relações empregatícias (subordinadas) quanto às autônomas e outras modalidades (PJ, plataformas, terceirizados), mesmo quando o trabalhador atua por meio de pessoa jurídica. A distinção está na **intensidade da aplicação dos princípios** (finalidade, necessidade, não discriminação, prestação de contas).
- **Hipóteses Legais:** Em relações subordinadas, o **consentimento é mais frágil** devido à assimetria. As bases mais comuns são **obrigação legal e legítimo interesse**. Em relações autônomas, o consentimento tem mais espaço, desde que livre e informado.
- **Fase Pré-Contratual:** Destacou o desafio do "**direito à explicação**" para candidatos preteridos, questionando se a negativa de contratação constitui um dado pessoal e gera

direito de acesso às deliberações. A transparência e critérios objetivos no recrutamento são essenciais para mitigar riscos.

- **Monitoramento e Vigilância (Boss Ware):** Abordou a tendência crescente do uso de sensores e IA para monitorar produtividade, emoções (análise facial), uso de EPI, etc.  
Concluiu que, tanto para empregados quanto para autônomos, a **legitimidade do monitoramento está atrelada a uma finalidade benéfica e proporcional**, como saúde e segurança do trabalho, e à **transparência prévia**.  
Em relações subordinadas, pode derivar do **poder diretivo do empregador** (desde que justificado). Para autônomos, depende de **previsão contratual clara**. Alertou para riscos de **discriminação algorítmica** e a necessidade de "sindicância dos algoritmos".
- **Fase Pós-Contratual:** Mencionou jurisprudência emergente sobre o **direito ao esquecimento/desindexação** (ex.: remover de sites de busca o vínculo empregatício passado).
- **Conclusão:** A palavra-chave é **boa-fé**. A aplicação da LGPD será cada vez mais tranquila à medida que se respeitem a finalidade legítima, a transparência e se garanta um **núcleo duro de opacidade** (direitos indisponíveis) ao trabalhador.

## 2. EXPOSIÇÃO – DRA. VOLIA BOMFIM

**Tema Central:** A necessidade de tratamento diferenciado para diferentes categorias de trabalhadores (empregados CLT, servidores públicos, autônomos) nas fases pré, durante e pós-contrato.

- **Diferenciação de Categorias:** A autonomia da vontade varia drasticamente. É quase nula para **servidores públicos** (estatutários), muito limitada para **empregados CLT** e maior para **trabalhadores autônomos**. Essa gradação deve orientar a análise das bases legais e do consentimento.
- **Fase Pré-Contratual:**  
Coleta deve se restringir a dados **essenciais e específicos** ao cargo.  
**Entidades de tendência** (ex.: loja que vende para um público específico) podem justificar coleta de dados sensíveis (como etnia), mas como exceção.  
**Exames médicos e psicológicos admissionais** só são permitidos quando expressamente autorizados por lei/NR (ex.: aeronautas, trabalhos em altura/espço confinado). A regra geral é a proibição.  
**Pesquisa de antecedentes criminais** é exceção; **pesquisa patrimonial** (Serasa) é vedada.
- **Grande Desafio Atual: A Norma Regulamentadora NR 1 (Fatores Psicossociais):**  
O questionário do censo para mapear riscos psicossociais invade a intimidade (ex.: uso de remédios, ideação suicida).  
Propôs **boas práticas críticas:** aplicação por terceiro (não pelo empregador), **anonimato** nas respostas, direcionamento voluntário para tratamento.
- **Inteligência Artificial no Trabalho:** Reforçou a importância do **direito à revisão humana** de decisões automatizadas (seleção, promoções) devido aos vieses discriminatórios inerentes aos algoritmos.
- **Fase Contratual e Compartilhamento de Dados:**  
O **compartilhamento** é um dos maiores pontos de angústia (ex.: com sindicatos, planos de saúde, empresas terceirizadas).

Defendeu que o compartilhamento com **sindicatos** para cobrança de contribuição **prevista em norma coletiva** configura **obrigação legal**, não mero legítimo interesse.

- **Fase Pós-Contratual e Prazos:** Alertou que é **impossível fixar um prazo único** para descarte de dados, devido aos prazos prescricionais trabalhistas variados (ex.: 2 anos para verbas, 5 anos para FGTS, 20 anos para ações de saúde). A **pseudonimização** foi sugerida como alternativa.
- **Judiciário como Empregador e Gestor de Processos:**  
Como empregador de servidores, o Judiciário deve cumprir a LGPD integralmente.  
Nos processos trabalhistas, defendeu a **mitigação de riscos**: sigilo para dados sensíveis das partes (doenças) e **pseudonimização** (iniciais) em publicações de diários oficiais e salários para balancear transparência e proteção.

### 3. DEBATE E ENCERRAMENTO

- O Conselheiro **Cassio Borges** agradeceu as contribuições, destacando que cobriram as principais angústias do GT, especialmente a análise por fases (pré, durante, pós) e a diferenciação entre tipos de vínculo, o que facilitará a estruturação do trabalho no eixo de princípios e bases legais.
- A Coordenadora **Debora Sirotheau** reforçou a riqueza das apresentações e citou como exemplo de caso prático relevante o **acesso de sindicatos aos dados de contato dos trabalhadores** (como e-mails) em cenários de trabalho híbrido/remoto, tema polêmico que merece aprofundamento.
- Ficou acordado que as especialistas disponibilizariam o material das apresentações e outros documentos (como livro da Dra. Volia) para anexação ao relatório final do GT, enriquecendo o subsídio a ser entregue à ANPD.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

#### ATA DE ENTREVISTA

**Data:** 02/02/2026

**Horário:** 16:00 as 17:52

**Participantes:** Débora Sirotheau Siqueira Rodrigues, Cassio Augusto, Alexandre Boava, Ana Rita Biba, Gaudio Ribeiro

---

#### ENTREVISTADOS: GÁUDIO RIBEIRO E ANA RITA

**GAUDIO RIBEIRO:** Professor e Mentor. Diretor-Presidente do Instituto DIA. Advogado com atuação destacada perante TST e STF. Ex-assessor de ministros no TST.

**ANA RITA:** CIPM | CDPO BR | Advogada da Opice Blum Advogados Associados

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

### Apresentação de Ana Rita:

Abordou os **Eixos 1 e 2** do questionário do CNPD, focando em:

**Princípios da LGPD aplicados ao trabalho:** Finalidade, Necessidade, Transparência.

**Bases legais no contexto laboral:** Consentimento (vulnerável pela assimetria de poder), Legítimo Interesse, Cumprimento de Obrigação Legal e Execução de Contrato.

**Importância do Aviso Interno de Privacidade:** Deve ser claro, adaptado ao público interno, de fácil acesso e acompanhado de comunicação ativa.

**Monitoramento:** Quanto mais intrusivo, maior a necessidade de transparência e justificativa proporcional.

Utilizou exemplos de diretrizes internacionais (GDPR, ICO/UK, CNIL/FR) e do TST (exigência de antecedentes criminais).

Concluiu que a LGPD, embora não tenha capítulo específico para trabalho, exige rigor redobrado devido à vulnerabilidade do trabalhador.

### Apresentação de Gaudio Ribeiro:

- Complementou com uma perspectiva **trabalhista e jurisprudencial**.
- Destacou que o **consentimento deve ser exceção** nas relações assimétricas, privilegiando outras bases legais.
- Apontou o **aumento significativo de reclamações trabalhistas** envolvendo a LGPD.
- Citou **jurisprudência do TST e TRTs** sobre temas como: controle biométrico, monitoramento de e-mails corporativos, geolocalização e sigilo de dados sensíveis em processos.
- Sugeriu a **negociação coletiva** como instrumento importante para tratar questões complexas, com documentação robusta do processo negocial.
- Enfatizou a necessidade de **diretrizes claras (soft law)** para dar segurança jurídica, evitando novas obrigações legais rígidas.

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**

Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPD

## ATA DE ENTREVISTA

Data: 09/02/2026

Horário: 16:00 as 17:26

Participantes: Débora Sirotheau Siqueira Rodrigues, Kamilla Mariana, Alexandre Boava.

---

ENTREVISTADA: SELMA CARLOTO

EDPO (certificada Exin), Professora da FGV de MBA e pós, Palestrante, Mestre Direito USP, Doutora Engenharia A UFABC e Direito UBA Pós-Doutora em Direito pela UFRGS.

---

As declarações aqui registradas refletem exclusivamente a percepção da entrevistada e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

Selma Carloto estruturou sua apresentação a partir de casos concretos vivenciados em sua atuação profissional, diagnosticando as falhas mais recorrentes na adequação de empresas à LGPD no âmbito das relações de trabalho. Seu ponto de vista é crítico e pragmático, lastreado em evidências empíricas e no direito comparado.

### 1. Diagnóstico Geral: O Erro Básico e Recorrente

**Ponto central:** A imensa maioria das empresas brasileiras **não possui sequer o básico** em matéria de proteção de dados para empregados.

**Caso emblemático – PricewaterhouseCoopers (Grécia):** Sancionada pela autoridade grega por tratar todos os dados de empregados sob a base do consentimento, sem aviso de privacidade específico. Selma usou este caso para ilustrar que "se uma empresa como a Price caiu nesse erro, imaginem as demais".

- **Três perfis de empresas diagnosticados:**

**Sem qualquer assessoramento:** Contabilidade ou RH insere cláusula genérica de consentimento no contrato de trabalho, achando que isso é "adequação à LGPD".

**Com adequação parcial e superficial:** Focam apenas em clientes/consumidores (aviso de privacidade no site, política de cookies), mas ignoram completamente os empregados.

**Com algum nível de assessoria, mas ainda com erros graves:** Fazem termos de consentimento separados, porém genéricos e cumulativos (várias finalidades em um único termo), ou confundem acordo de confidencialidade com consentimento.

**Entendimento de Selma:** *"A empresa está em pior conformidade com essa cláusula de consentimento no contrato do que se não tivesse nada."* O documento errado agrava o risco, pois cria uma falsa sensação de segurança e não resiste a qualquer fiscalização ou questionamento judicial.

## 2. Consentimento no Contexto Laboral: Exceção, Não Regra

**Tese central:** O consentimento não é e não pode ser a base legal primária nas relações de trabalho. Deve ser reservado a tratamentos genuinamente opcionais, sem qualquer prejuízo ou penalização pela recusa.

- **Fundamentos:**

Assimetria de poder e dependência econômica viciam o consentimento.

Leis comparadas (ex.: Portugal, Lei n. 58/2019) preveem expressamente que o consentimento do trabalhador não constitui requisito de legitimidade, salvo quando dele resulte vantagem jurídica ou econômica – hipótese em que, justamente por isso, não poderia ser utilizado, pois a vantagem descaracteriza a liberdade.

- **Exemplos corretos de uso do consentimento:**

Participação voluntária em campanha de endomarketing (vídeos, fotos para site/intranet).

Filmagem eventual em que o empregado pode ser realocado para outro local sem prejuízo.

- **Exemplos incorretos (e recorrentes):**

Consentimento forçado em plataformas de recrutamento e seleção: o candidato é obrigado a aceitar compartilhamento de dados para continuar a inscrição.

Aplicativo de contracheque que exige consentimento para ofertas de consignados e produtos como condição para acesso ao holerite.

Exame de gravidez na dispensa tratado sob consentimento – Selma defende, com base em artigo de sua autoria (2021), que a base correta é legítimo interesse, pois há vantagem econômica e proteção ao nascituro.

## 3. Aviso de Privacidade para Empregados: O Grande Ausente

**Diagnóstico:** Selma afirmou que, em toda sua experiência como consultora, jamais encontrou uma empresa que já tivesse um aviso de privacidade específico para empregados no início dos trabalhos.

- **Consequências:** Sem transparência, o trabalhador não sabe quais dados são tratados, para quais finalidades, com quem são compartilhados, por quanto tempo são retidos, nem como exercer seus direitos.
- **Boa prática sugerida:** Aviso de privacidade em formato de tabela (finalidade, dados tratados, base legal, compartilhamento), nos moldes da recente resolução da ANPD. Didático, claro e acessível.
- **Erro comum:** Achar que o aviso de privacidade do site (clientes/consumidores) supre a necessidade dos empregados.

#### 4. Legítimo Interesse e Monitoramento: Onde Estão os Maiores Riscos

**Entendimento:** O legítimo interesse é a base legal mais recorrente para tratamentos críticos (monitoramento, videovigilância, geolocalização, verificação de antecedentes criminais fora das hipóteses legais estritas), mas é também a mais mal aplicada.

- **Problemas identificados:**

Ausência de teste de balanceamento (LIA) ou testes superficiais, "mascarados".

- o tratamento excessivo e desproporcional: softwares que capturam imagens, tudo o que é digitado, telas, etc., sem necessidade real para a finalidade declarada.

Exemplo crítico: software de monitoramento de produtividade (caso análogo ao citado no guia da ANPD e no parecer 2/2017 do WP29). Selma enfatizou: *"Não passa na etapa 2 do teste de balanceamento."*

- **Recomendação:** Empresas devem priorizar os tratamentos de maior risco (monitoramento, videovigilância) para elaboração de LIAs robustos.

#### 5. Antecedentes Criminais: Finalidade Legítima vs. Discriminação

**Posição de Selma:** A consulta a antecedentes criminais não é proibida, mas deve ser justificada e proporcional.

- **Hipóteses legítimas:**

Escolas, creches, lares de idosos (proteção de vulneráveis).

Trabalhadores com acesso a informações sigilosas, armas, perfurocortantes, substâncias controladas, transporte de valores.

- **Erro comum:** Pesquisar antecedentes criminais para qualquer vaga, inclusive administrativas, sem qualquer correlação com as atribuições.

- **Outras pesquisas ilícitas recorrentes:**

Consulta a órgãos de proteção ao crédito (SPC, Serasa) para fins de contratação.

Consulta a processos trabalhistas.

Coleta de certidões de casamento, nascimento de filhos, cópias de RG, mesmo após os dados já terem sido inseridos em sistemas.

#### 6. Outras Falhas Graves e Recorrentes

- **DPO em conflito de interesses:** Nomeação de gerentes de TI, jurídico ou RH como encarregado, sem afastamento das funções originais. Selma citou guia da ANPD sobre conflito de interesses e sua própria produção acadêmica sobre o tema.
- **ROT (Registro de Operações de Tratamento) deficiente:** Não reflete a realidade da área trabalhista; subnotificação de atividades.
- **Prazos de retenção:** Empresas mantêm atestados médicos físicos por décadas, sem política de descarte, com risco físico (incêndio, extravio) e jurídico.
- **Coleta excessiva na contratação:** Documentos que não guardam relação com a função ou já foram digitalizados permanecem armazenados fisicamente sem necessidade.

## 7. O Problema Estrutural dos Grandes Fornecedores

Alexandre Boava corroborou o diagnóstico de Selma e aprofundou a questão das grandes plataformas de tecnologia (Microsoft, Google, Oracle, AWS, Atlassian etc.).

- **Ponto central:** Essas empresas, na prática, impõem suas políticas de privacidade e modelos de consentimento aos controladores (empregadores), que não têm poder de barganha para alterá-las.
- **Consequência:** O empregador se vê obrigado a repassar ao empregado condições que sabidamente não estão em conformidade, sob pena de não acessar serviços essenciais.
- **Reflexão:** Em muitos casos, o operador (grande plataforma) atua como co-controlador, pois toma decisões sobre o tratamento sem seguir as instruções do controlador contratante.

Selma complementou que já solicitou, por escrito, adequações a essas empresas, com a resposta de que "não têm interesse em ajustar", assumindo o risco e, juridicamente, a posição de controladoras (art. 42, LGPD).

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPD

### ATA DE ENTREVISTA

**Data:** 23/02/2026

**Horário:** 16:00 as 17:18

**Participantes:** Débora Sirotheau Siqueira Rodrigues,

---

**ENTREVISTADA:** Tatiana Bhering Roxo

Advogada | Consultora em Direito do Trabalho, Proteção de Dados e Digital | Estratégia Jurídica para Negócios com Segurança e Clareza.

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

Tatiana estruturou sua apresentação a partir de uma **visão integrada entre a LGPD e o Direito do Trabalho**, defendendo que muitas respostas para os desafios da proteção de dados nas relações laborais já existem na legislação e jurisprudência trabalhistas, carecendo apenas de uma **adaptação cultural e de governança**. Seu ponto de vista é **pragmático e fundamentado na experiência do dia a dia do RH e das relações sindicais**.

## 1. Finalidades do Tratamento e Princípio da Necessidade

**Diagnóstico:** As finalidades nas relações trabalhistas são, em regra, legítimas e específicas, pois a relação de emprego exige tratamento de dados (ex.: eSocial). O problema reside na **aplicação prática**, com perpetuação de práticas pré-LGPD.

### Pontos críticos identificados:

- **Falta de governança de dados no RH:** Empresas investem em conformidade para clientes/consumidores, mas **negligenciam os dados dos próprios empregados**, onde reside o maior risco.
- **Coleta excessiva e desproporcional:** Formulários genéricos com campos desnecessários (inclusive de familiares) são mantidos por inércia.
- **Problemas com plataformas terceirizadas de RH:** Fornecedores resistem a customizar formulários, e o empregador, sem poder de barganha, repassa ao empregado a instrução informal de "não preencher", o que é ineficaz diante da assimetria de poder.
- **Segmentação necessária:** Empresas com perfis diversos de trabalhadores (chão de fábrica vs. escritório) não podem usar o mesmo formulário padronizado.

**Recomendação prática:** Dividir a análise por **fases da relação** (pré-contratual, contratual, pós-contratual) para organizar a governança e definir finalidades proporcionais.

## 2. Consentimento no Contexto Laboral

**Tese central:** O consentimento deve ser **absolutamente excepcional** e jamais inserido em contrato de trabalho (que é contrato de adesão), sob pena de nulidade.

### Critérios para uso legítimo do consentimento:

1. **Finalidade lícita e proporcional:** Deve ser algo **genuinamente opcional**, sem qualquer relação com a execução do contrato ou obrigação legal.
2. **Informação efetiva:** Linguagem acessível ao destinatário (trabalhador).
3. **Liberdade real:** A recusa não pode gerar qualquer consequência negativa, retaliação ou constrangimento (exemplo: mural de aniversariantes que pode gerar *bullying* indireto).

4. **Convergência com interesse do empregado ou indiferença:** A pessoa só consente livremente se houver algum benefício para si ou se a situação lhe for completamente indiferente (ex.: filmagem eventual com possibilidade de realocação).
5. **Granularidade:** O consentimento deve ser por finalidade específica, nunca genérico.
6. **Revogação possível e sem retaliação:** O direito de revogar deve ser tão livre quanto o de consentir, inclusive se o contexto da relação mudar (ex.: mudança de liderança).

**Exemplo prático correto:** Campanha de Dia dos Pais/Dia das Mães com pedido de foto ou depoimento voluntário.

### 3. Legítimo Interesse: Ponderação e Limites

**Entendimento:** O legítimo interesse é base legal relevante no contexto laboral, mas exige **teste de balanceamento rigoroso** (legitimidade, necessidade, equilíbrio).

#### Aplicação prática:

- **Legitimidade:** A mera existência da relação de emprego **não basta** para justificar qualquer tratamento. É preciso finalidade concreta (ex.: monitoramento só se houver risco real a ser protegido).
- **Necessidade:** Deve-se verificar se há alternativa menos invasiva (ex.: controle de jornada: empresa com 20 empregados não precisa de biometria; com 5.000, talvez faça sentido).
- **Balanceamento:** Ponderar interesse econômico da empresa vs. direitos fundamentais do trabalhador.
- **Salvaguardas:** Transparência reforçada, oposição facilitada, medidas de segurança, e, se for o caso, Relatório de Impacto (RIPD).

**Exemplo de uso inadequado:** Compartilhar e-mails dos empregados com terceiros para ofertas não relacionadas ao contrato de trabalho.

### 4. Execução do Contrato e Obrigação Legal: Bases Centrais, mas com Limites

#### Pontos centrais:

- **Obrigação legal:** É a base mais segura. Exige mapeamento completo do arcabouço normativo aplicável à empresa (leis, NRs, normas coletivas) para delimitar finalidades e dados estritamente necessários.
- **Execução do contrato:** Mais delicada, pois o "papel aceita tudo" e o empregado hipossuficiente tende a aceitar cláusulas abusivas. Exige **juízo de ponderação** entre poder empregatício e direitos fundamentais.
- **Minimização de dados:** Deve ser princípio norteador em todas as bases.

**Exemplo crítico:** Uso da biometria para controle de jornada. Tatiana defende análise contextual: empresas sem obrigação legal de controle de ponto (menos de 20 empregados) não deveriam usar biometria, pois há alternativas menos invasivas. Já para grandes plantas fabris, pode ser justificável, desde que com salvaguardas.

## 5. Transparência e Direitos dos Titulares

**Diagnóstico contundente:** Avisos de privacidade para empregados são **raríssimos** na prática. O que existe é voltado a clientes/consumidores.

### Problemas identificados:

- Avisos genéricos anexados ao contrato de trabalho, nunca mais atualizados ou comunicados.
- Canais de comunicação inadequados: empregados recorrem ao RH, mas o encarregado é direcionado a clientes.
- Falta de linguagem acessível: avisos em juridiquês, incompreensíveis para o público interno, especialmente em fábricas.

### Recomendações práticas:

- Adaptar a comunicação ao perfil do trabalhador (mural, plataforma interna, vídeos curtos, linguagem simples).
- Integrar o RH ao encarregado: o RH deve ser o canal de contato, com suporte técnico do DPO.
- Seguir a lógica da **Recomendação da OIT de 1997** (ainda atual): informação regular, acesso em horário de trabalho, direito de examinar e obter cópias.
- Lembrar que, em eventual disputa judicial, o documento formal sem efetiva comunicação é considerado inexistente (primazia da realidade).

## 6. Monitoramento, Vigilância e Tecnologias de Produtividade

**Tese central:** O poder empregatício encontra limites nos direitos fundamentais. Monitoramento só é legítimo se:

- Finalidade legítima e explícita.
- Limitado ao espaço e tempo de trabalho.
- Proporcional e com minimização de dados.
- Comunicado previamente de forma clara.

### Riscos identificados:

- **Vigilância panóptica e adoecedora:** Monitoramento excessivo (tempo ativo de tela, velocidade de resposta, duração de pausas) gera discriminação e sofrimento mental, especialmente para PcDs, pessoas com restrições de saúde ou responsabilidades familiares.
- **Geolocalização invasiva:** Quando não limitada ao horário de trabalho ou quando o veículo é usado também para fins pessoais (benefício) e o monitoramento não é desligado.
- **Distribuição algorítmica de tarefas:** Pode marginalizar trabalhadores menos bem avaliados, impedindo seu desenvolvimento.
- **Uso secundário de dados:** Coletar para uma finalidade e usar para outra (ex.: análise de currículos para estudo de mercado, perfilamento).

#### **Discriminação algorítmica:**

- **Discriminação indireta:** Exemplo clássico do software da Amazon que excluía currículos de mulheres por "aprender" com padrões históricos masculinos.
- **Necessidade de auditoria e gestão de terceiros:** Empresas precisam auditar ferramentas contratadas para garantir explicabilidade e não discriminação.

**Proposta:** Incorporar princípios de "**Fair Work for AI**" (Carlos Kant, Oxford): trabalho decente, transparência, equidade, ética digital, segurança, criação de empregos, impacto positivo.

## **7. Negociação Coletiva e Participação dos Trabalhadores**

**Posição de Tatiana:** A negociação coletiva é **o caminho mais adequado** para tratar desses temas, por ser mais ágil que a lei e capaz de trazer segurança jurídica.

#### **Desafios atuais:**

- Cláusulas genéricas e superficiais ("as partes se comprometem a cumprir a LGPD").
- Resistência das empresas em fornecer informações aos sindicatos, alegando (erroneamente) sigilo da LGPD.
- Enfraquecimento das entidades sindicais (crise de representatividade, fim da contribuição obrigatória).
- Baixa prioridade do tema diante de problemas trabalhistas mais urgentes (jornada, assédio).

#### **Propostas:**

- Institucionalizar a participação: prever em lei ou norma a consulta prévia a sindicatos ou comissões paritárias para implementação de tecnologias de monitoramento e IA.
- Criar **guias ou roadmaps oficiais** (ex.: provimento do CNJ para cartórios) que orientem a governança e possam ser adotados em normas coletivas.

- Estimular cláusulas específicas sobre: finalidades legítimas, bases legais adequadas, transparência, direitos dos titulares, auditoria de algoritmos.

**Exemplo positivo:** O Decreto da Transparência da Itália exige procedimentos compartilhados para ferramentas digitais de gestão algorítmica.

## 8. Capacitação e Campanhas Educativas

**Entendimento:** A mudança cultural passa por **treinamento obrigatório e recorrente**, nos moldes das NRs (ex.: NR-1, NR-5).

### Recomendações:

- Exigir periodicidade, carga horária e conteúdo mínimo em campanhas educativas sobre proteção de dados.
- Adaptar a linguagem ao público-alvo (ex.: previdência privada vs. agência de publicidade).
- Medir a efetividade da compreensão.
- Incluir metas de proteção de dados para líderes (assim como já se tenta com sustentabilidade).

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

### ATA DE ENTREVISTA

**Data:** 16/03/2026

**Horário:** 16:00 as 17:07

**Participantes:** Débora Sirotheau Siqueira Rodrigues,

---

**ENTREVISTADA: Priscila Zoghbi**

**Phd em Direito do Trabalho na Universidade de São Paulo**

---

As declarações aqui registradas refletem exclusivamente a percepção dos entrevistados e não devem ser interpretadas como posicionamento institucional.

Sumário executivo da visão da entrevistada:

A discussão especializada em direito laboral com Priscila Zoghbi analisou a vida útil dos dados do empregado celetista, focando na assimetria de poder e na insuficiência da base legal de consentimento diante dos desafios impostos pelas Big Techs.

Os principais aspectos abordados pela entrevistada foram:

- **Introdução da Especialista e Definição da Abordagem:** Priscila Zoghbi se apresentou como especialista em direito do trabalho, com formação na USP e estudos de pós-doutorado em Portugal e Milão sobre direito laboral, inteligência artificial e tecnologia. Ela propôs que a sessão fosse conduzida como um bate-papo focado nas dúvidas dos participantes para que o conteúdo fosse mais produtivo e para que Priscila pudesse adicionar valor ao que já vinha sendo discutido em sessões prévias.
- **Contexto da Proteção de Dados no Âmbito Laboral:** Alexandre Boava destacou a ausência de um documento oficial da agência nacional de proteção de dados que oriente especificamente a situação da proteção de dados no contexto laboral. Eles notaram que o dado do trabalhador enfrenta questões econômicas significativas e segue um trâmite distinto de outros titulares de dados.
- **Desafios da Economia de Dados e Fornecedores de Tecnologia:** A missão principal do grupo é estabelecer o que é coerente e juridicamente correto fazer com o dado do trabalhador, especialmente em relação a como o empregador lida com fornecedores de plataformas, sobretudo Big Techs. Muitas empresas brasileiras sentem-se obrigadas a utilizar grandes plataformas para serviços em nuvem ou de operação, o que as força a submeter seus trabalhadores aos termos de uso e políticas de privacidade desses fornecedores.
- **Monitoramento e Uso de Dados do Trabalhador:** Os dados dos trabalhadores incluem informações cadastrais (nome, endereço) e dados da atividade laboral (horário de entrada/saída, velocidade de trabalho), indo ao encontro do paradigma da monitoria no home office. Esses dados são frequentemente usados para aprimorar produtos, plataformas e criar novos serviços de consultoria para empregadores, solidificando o papel das empresas de tecnologia como intermediadoras entre empregados e empregadores.
- **Modelos de Trabalho Plataformizados e Dados Sensíveis:** O modelo plataformizado se expandiu para diversas funções (médico, psicólogo) e a relação de trabalho nessas plataformas não possui a proteção da CLT. Nesses contextos, dados sensíveis, como informações de saúde, são envolvidos, e há dificuldades em fazer valer a LGPD, conforme documentado pelo Ministério Público do Trabalho (MPT), especialmente em relação ao artigo que exige explicação sobre decisões automatizadas.
- **Proposta de Recorte Focado em Empregados CLT:** Priscila Zoghbi sugeriu um recorte inicial para focar a discussão apenas no "empregado" (aquele submetido à CLT), pois a quantidade de temas abertos tornava a discussão muito ampla. O objetivo era garantir que o encontro fosse produtivo e que os participantes pudessem extrair pontos concretos para a discussão.
- **Estrutura Documental e Eixos de Análise:** Cassio Augusto Borges confirmou que o material de referência do grupo estava estruturado em quatro eixos, sendo eles um

começo para a estruturação do documento final. Ele é responsável pelo eixo de "princípios e bases legais" e mencionou a carência de uma orientação oficial (como um guia) da Agência Nacional.

- **Distinção entre Trabalhador e Empregado sob LGPD:** Cassio Augusto Borges reforçou a importância da distinção entre trabalhador lato sensu e empregado stricto sensu (celetista), pois a incidência normativa da LGPD pode ser diferente para cada um. Ele também mencionou o modelo de análise tripartite da relação laboral: fase pré-contratual, contratual e pós-contratual.
- **Análise das Fases da Relação Laboral:** A fase pré-contratual envolve seleção e recrutamento, exigindo verificação de princípios, bases legais e descarte de dados. O período pós-contratual gera dúvidas sobre o tempo de guarda e descarte de documentos, especialmente em face da prescrição trabalhista ou de decisões recentes do TST.
- **Origem da LGPD e o Efeito Bruxelas:** Priscila Zoghbi introduziu a análise da Lei Geral de Proteção de Dados (LGPD) sob a perspectiva de sua origem, que veio de um movimento global influenciado pelo Regulamento Europeu (GDPR). Esse movimento global é impulsionado pelo "Efeito Bruxelas", onde regulamentos produzidos pela União Europeia, como o GDPR, influenciam outros países a criarem suas próprias leis para garantir o acesso ao mercado consumidor europeu.
- **Abordagem da LGPD por Princípios e Evitando Especificidades Tecnológicas:** A LGPD brasileira não possui um artigo específico sobre o direito do trabalho sob a CLT, e o GDPR tem apenas um. Devido à rápida obsolescência das tecnologias (como o exemplo do fax), Priscila considera positivo que a lei não se prenda a tecnologias específicas, sugerindo que o foco deve ser nos princípios, como o da necessidade.
- **Análise da Vida Útil do Dado do Empregado em Três Momentos:** Priscila propôs dividir a análise da vida útil do dado do empregado em três momentos. O primeiro é a coleta, frequentemente marcada por problemas como coleta excessiva de dados não vinculados à performance do contrato. Os outros momentos são a manutenção do contrato e o pós-contratual.
- **Uso do Consentimento como Última Base Legal:** Priscila sugeriu que o consentimento deve ser a última base legal a ser utilizada para o tratamento de dados do empregado, devido à assimetria de poder na relação laboral. Bases preferenciais incluem a performance contratual (necessidade dos dados para pagamento ou execução do trabalho) e o cumprimento de obrigação legal.
- **Desafios e Soluções na Fase Pré-Contratual:** Problemas na fase pré-contratual incluem a coleta preventiva de informações e a falta de transparência sobre a retenção dos dados. Soluções propostas incluem a criação de frentes de educação e instrução para empregados e empregadores, fiscalização, e a adoção de coletas graduais ou em camadas.
- **Transparência e Consentimento na Retenção de Currículos:** Em casos de não contratação, a falta de transparência sobre o destino do currículo é um problema, pois o dado pode ser mantido ou repassado a terceiros (como empresas de RH) sem o conhecimento do candidato. O dever de transparência exige que se formalize um instrumento opcional (diferente da candidatura) onde o empregado consinta com a manutenção do currículo por um prazo definido.

- **Diferenciação entre Consentimento e Vontade de Obter o Emprego:** Em resposta a Cassio, Priscila esclareceu que consentimento é diferente da vontade de obter o emprego, que motiva o envio do currículo. O consentimento torna-se a base legal para o tratamento dos dados (como o tempo de retenção no banco de dados) e não para a simples submissão do currículo para a vaga.
- **Uso da Performance Contratual na Fase Pré-Contratual:** Priscila sugeriu que, na fase pré-contratual (mesmo sem contrato de trabalho formalizado), a base legal para o tratamento dos dados necessários pode ser a performance do contrato, ou seja, o que é necessário para a execução do propósito. O uso do princípio da necessidade ou minimização de dados deve limitar o empregador a questionamentos estritamente relacionados à vaga.
- **Controle de Acesso e Governança Corporativa de Dados:** Um problema recorrente nas empresas é a falta de controle de acesso aos dados, onde muitas vezes a própria empresa não sabe quem está acessando as informações. A sugestão é aplicar sistemas de camadas (etapas) para que apenas as pessoas estritamente necessárias tenham acesso aos dados, dependendo da fase (pré-contratual ou contratual).
- **Fase Pós-Contratual e Limitação de Retenção:** A fase pós-contratual é considerada menos problemática, pois a base legal é geralmente a obrigação legal (retenção para fins fiscais ou possíveis reclamações trabalhistas). No entanto, a retenção ilimitada de dados, assim como o monitoramento ilimitado, fere a dignidade da pessoa humana e deve ser limitada.
- **Princípios Interligados e Análise Comparativa de Casos:** Priscila enfatizou que os princípios da LGPD (como a necessidade) são interligados e devem permear toda a vida útil do dado do trabalhador. Ela recomendou analisar casos julgados pela Corte Europeia, como o caso Barbaresco, que servem como referência para sistemas de balanceamento de monitoramento, mas sem aplicar um "copia e cola" ao direito brasileiro.
- **Ausência de Proteção Específica ao Trabalhador na LGPD/GDPR:** Priscila reformulou seu ponto sobre a LGPD, afirmando que a ausência de referência a tecnologias específicas não é de todo ruim (devido à rápida evolução tecnológica). Contudo, a ausência de referência e proteção específica ao trabalhador é considerada uma grande falha tanto na LGPD quanto no GDPR.
- **Dificuldade de Implementação do Privacy by Design:** O modelo de Privacy by Design e Privacy by Default é recente e de difícil interpretação e análise. A implementação rigorosa desses modelos forçaria as Big Techs a refazerem bases de dados e algoritmos, o que envolveria grande perda de investimento, configurando uma questão de poder e de contradição com o modelo de negócio dessas empresas.
- **Falta de Controle e Cultura de Segurança de Dados nas Empresas:** Foi observado que há uma falta de controle e de uma cultura de segurança em relação a quem acessa os dados dentro das empresas, pois essa não é uma prioridade. O letramento e acultramento do trabalhador são vistos como importantes para que eles possam interferir na situação.
- **Problema Crônico de Golpes e Vazamento de Dados:** Alexandre Boava destacou que há um problema crônico de golpes cada vez mais sofisticados, que utilizam dados pessoais e de comportamento online. Eles observaram que as informações estão vazando,

e que o tratamento de dados dentro de empresas de consultoria permite uma grande facilidade para fazer o que se quiser com essas informações, existindo até um mercado para isso. Eles concordaram que recebem muitas ligações aleatórias, um sintoma do vazamento de dados.

- **Acumulação Preventiva de Dados e Latifúndios Digitais:** A Priscila Zoghbi mencionou uma experiência em um hospital onde dados de pacientes eram acessíveis por todos os setores ("todo mundo ticado") sob a justificativa de "vai que precisa". Eles argumentaram que essa coleta preventiva e excessiva de dados transforma os usuários em "acumuladores". Alexandre denominou chamou essa prática, no contexto de seu movimento, de criação de "latifúndios de dados" que ficam parados, esperando o momento certo para serem valorizados, seguindo uma lógica de especulação imobiliária.
- **Pesquisa Acadêmica sobre Datificação do Trabalho e Google Docs:** Alexandre Boava, que também é pesquisador, compartilhou que está no mestrado estudando a datificação da atividade de trabalho de comunicadores em plataformas de trabalho coletivo, focando especificamente no Google Docs. Eles desenvolveram uma extensão para entender como o Google Docs se apropria dos dados, conversando com os servidores, e iniciaram o projeto como apoio técnico. A sua pesquisa visa entender a economia de dados.
- **Apropriação e Condicionamento de Dados por Aplicativos:** Alexandre usou o exemplo de um aplicativo de lanterna cuja função é operacionalizar a câmera, mas que condiciona o usuário a ceder acesso à sua lista de contatos e fotos. Essa prática é sintomática da situação atual, onde toda oportunidade de datificação está sendo apropriada e condicionada em contratos. A Priscila Zoghbi levantou a questão jurídica do consentimento, mencionando que vincular a funcionalidade principal do aplicativo ao compartilhamento de contatos (consentimento condicionado) pode gerar problemas jurídicos, especialmente em auditorias internacionais.
- **Análise dos Termos de Uso das Big Techs:** Alexandre mencionou uma análise de discurso que fizeram dos termos de uso das big techs, onde concluiu-se que qualquer coisa que tenha finalidade operacional será usada para pegar todos os rastros do usuário. Eles observaram que, no limite, o indivíduo vive em uma economia onde nem mesmo o seu celular é de fato dele, e que nada é realmente seu, exceto o "amor de mãe".

Fim dos registros.

**Débora Sirotheau Siqueira Rodrigues**  
Coordenadora do GT - Proteção de Dados no Contexto Laboral  
CNPd

## **Anexo 5 – Contribuições recebidas**



## **Contribuições Escritas**

## **Apresentações**