LTr Editora Ltda.

Rua Jaguaribe, 571
CEP 01224-003
São Paulo, SP — Brasil
Fone (11) 2167-1101
www.ltr.com.br
Maio, 2022

Produção Gráfica e Editoração Eletrônica: PIETRA DIAGRAMAÇÃO
Projeto de capa: DANILO REBELLO

Versão digital — LTr 9849.3 — ISBN 978-65-5883-147-1

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Carloto, Selma

Lei Geral da Proteção de Dados [livro eletrônico]: incluindo modelos, segurança da informação e fases de implementação / Selma Carloto. – 3. ed. – São Paulo: LTr, 2022. PDF

Bibliografia.

ISBN 978-65-5883-147-1

1. Proteção de dados – Direito – Brasil 2. Proteção de dados – Leis e legislação 3. Proteção de dados pessoais 4. Sistemas de informação gerencial - Medidas de segurança I. Título.

22-106183 CDU-342.721

Índice para catálogo sistemático:

1. Lei Geral de Proteção de Dados : Direito à privacidade 342.721

Cibele Maria Dias - Bibliotecária - CRB-8/9427

INTRODUÇÃO

Considerando que nossos dispositivos estão nos ouvindo e rastreando o tempo todo e tudo que estamos fazendo, como podemos manter nossos dados pessoais seguros? Como podemos proteger os dados dos trabalhadores e dos consumidores? A proteção e os cuidados com os dados pessoais, tornou-se uma questão inadiável. A principal preocupação da legislação brasileira de proteção de dados, assim como a do regulamento europeu, é exatamente proteger os dados das pessoas naturais, com a devolução do controle dos dados pessoais para seus titulares. A autodeterminação informativa, conceito que surgiu na Alemanha, é fundamento da Lei Geral de Proteção de Dados e consiste em garantir o controle do cidadão sobre suas próprias informações.

A tecnologia vem avançando em ritmo cada vez mais acelerado, nos conectamos cada vez mais digitalmente, os algoritmos de inteligência artificial dominam e influenciam o mundo, as pessoas, nas relações familiares, entre amigos, em relações de consumo e de trabalho, e vem sendo utilizada desde o processo seletivo em algumas empresas. Os algoritmos e métodos de inteligência artificial dependem de cálculo e estatísticas, sendo a máquina muito mais rápida e eficaz que o ser humano pensante, mas os riscos deverão ser sempre avaliados, principalmente se existe algum risco de desconformidade às normas de proteção de dados e à Constituição Federal, como vieses discriminatórios em um processo seletivo realizado por um robô.

A Lei n. 13.709/2018, denominada Lei Geral de Proteção de Dados, com as devidas alterações da Lei n. 13.853/2019, foi inspirada no Regulamento (UE) 2016/679 do Parlamento

Europeu de 27 de abril de 2016, o *General Data Processing Regulation*, ou Regulamento Geral sobre a Proteção de Dados.

O Regulamento Geral sobre a Proteção de Dados é um regulamento do direito europeu, que entrou em vigor no dia 25 de maio de 2018, sobre privacidade e proteção de dados pessoais e que é aplicável a todos os indivíduos da União Europeia e empresas que operem no Espaço Econômico Europeu, independente do país de origem e que revogou a Diretiva 95/46/CE. A Diretiva demandava que cada estado-membro aprovasse uma legislação interna adicional, já o regulamento é vinculativo e aplicável imediatamente a todos países da União Europeia, independentemente de adequação legislativa interna e garantindo o mesmo nível de proteção a todos países da União Europeia. A Diretiva havia sido escrita na fase inicial da internet, quando não eram conhecidos conceitos como internet das coisas, conectando o mundo físico ao digital por meio de objetos, *big data,* nuvem, inteligência artificial, *machine learning* e *deep learning,* não obstante esta já trouxesse conceitos importantes, bases legais de tratamento, diferença de dados pessoais e sensíveis, entre outros institutos e é por essa razão que os estudos do Grupo de Trabalho do Artigo 29, por esta criada, são tão importantes.

Se retrocedermos na história, o direito à privacidade foi consagrado pela primeira vez num instrumento jurídico internacional no artigo 12º da Declaração Universal dos Direitos do Homem", 1948: "Ninguém será sujeito a interferências na sua vida privada, família, lar ou na sua correspondência, nem a ataque à sua honra e reputação. Toda Pessoa tem direito à proteção da lei contra tais interferências ou ataques". A Declaração Universal dos Direitos do Homem influenciou a formulação de outros instrumentos sobre direitos humanos na Europa.

No final da II Guerra Mundial foi criado o Conselho da Europa, o qual reúne Estados da Europa com o objetivo de promover o Estado de direito, a democracia, os direitos humanos e o desenvolvimento social e o qual adotou a Convenção Europeia dos Direitos do Homem no ano de 1950 e que entrou em vigor em 1953. Em 1959, foi criado na França o Tribunal Europeu dos Direitos do Homem para garantir que as partes contratantes cumpram as obrigações assumidas ao abrigo da Convenção Europeia de Direitos do Homem e o qual se pronunciou, por meio de sua jurisprudência, em várias situações onde foi suscitada a proteção de dados.

O artigo 8º da Convenção Europeia de Direitos do Homem garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência, além de estabelecer as condições em que são permitidas restrições a este direito. O Comité de Ministros do Conselho da Europa logo adotou várias resoluções sobre a proteção de dados pessoais e que faziam referência ao artigo 8º da Convenção Europeia dos Direitos do Homem. Logo, foi aberta para assinatura a Convenção 108 de 1981, a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, no âmbito do Conselho da Europa e primeiro instrumento internacional juridicamente vinculativo, o qual regula expressamente a proteção de dados.

A Lei Geral de Proteção de dados do Brasil tem por objetivo garantir a transparência em todas as operações realizadas com os dados da pessoa natural, como a coleta, processamento, arquivamento, armazenamento, eliminação e compartilhamento dos dados pessoais.

A Lei Geral de Proteção de Dados brasileira tem por escopo resguardar os dados pessoais de seus titulares ou pessoas naturais, tanto nos meios digitais, como nos físicos,

devendo ser observada tanto pelas pessoas jurídicas de direito privado, quanto pelas de direito público.

Os avanços tecnológicos dos últimos anos, com as novas tecnologias da informação, vieram para alterar de forma permanente o mundo que nos rodeia e trouxeram a necessidade de uma legislação sólida de proteção dos dados das pessoas naturais, que buscasse o equilíbrio entre a garantia das liberdades e direitos individuais e que se traduz na reserva da intimidade da vida privada e a liberdade de circulação da informação pessoal:

> "A rapidez dos avanços tecnológicos e da globalização vieram para alterar de forma indelével o mundo que nos rodeia e são assim novos e imensos os desfechos para a proteção de dados. Os regimes de proteção de dados buscam o necessário equilíbrio entre dois princípios: por um lado, a garantia das liberdades e direitos individuais e, por outro lado, a liberdade de utilização e circulação da informação pessoal.
>
> (...)
>
> A verdade é que nos tornamos dependentes das comunicações móveis, do acesso instantâneo à informação e serviços inteligentes. Apesar de todos os benefícios dessas tecnologias, persistem dúvidas e preocupações sobre o quanto de informação pessoal é coligada, armazenada, utilizada e compartilhada para o fornecimento desses serviços persuasivos e convenientes."(1)

O Regulamento Geral de Proteção de Dados da União Europeia destaca, já no Considerando 1, que a proteção

(1) De MAGALHÃES, Márcia. *O Regulamento Geral de Proteção de Dados*. Porto: Librum Editora, 2019.

relacionada ao tratamento de dados pessoais das pessoas naturais é um direito fundamental previsto no artigo 8º, número 1, da Carta dos Direitos Fundamentais da União Europeia e no artigo 16º, número 1, do Tratado sobre o Funcionamento da União Europeia:

> "(1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, n. 1, da Carta dos Direitos Fundamentais da União Europeia ("Carta") e o artigo 16º, n. 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares."[(2)]

---

(2) GDPR EUROPA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679. Acesso em: 13 dez. 2020.

No Brasil, a Proposta de Emenda à Constituição Federal de 1988, número 17/2019, recentemente aprovada no Senado, acrescenta o inciso XII-A ao artigo 5º, e o inciso XXX ao artigo 22 da Constituição Federal de 1988, para incluir a proteção de dados pessoais, físicos e digitais, entre os direitos e garantias fundamentais do cidadão no Brasil e fixar a competência privativa da União para legislar sobre a matéria.

A Lei n. 13.709 de 14 de agosto de 2018 tem como fundamento a tutela aos **direitos fundamentais de liberdade e de privacidade**, **ao livre desenvolvimento da personalidade da pessoa natural e aos direitos humanos**:

> "Art. 1º Esta Lei dispõe sobre o **tratamento de dados pessoais, inclusive nos meios digitais,** por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de **proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural**.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei n. 13.853, de 2019)
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."(3)

(3) BRASIL. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <http://www.planalto.gov.br/cci-vil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 4 jan. 2022.

O escopo da presente legislação brasileira de proteção de dados é a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a qual é considerada vulnerável em relação aos agentes de tratamento, de forma a buscar-se um equilíbrio nas relações e aplicando-se a máxima da igualdade material, com base na justiça distributiva e compensatória.

Na era do *Big Data* e com um ambiente de globalização, o qual mitiga as fronteiras físicas, trazendo cada vez mais vantagens para o comércio eletrônico e com uma economia totalmente baseada na internet, cada vez mais dependente de dados, o escopo da proteção de dados pessoais é transformar o *Bid Data* em *Small Data,* devendo-se limitar o tratamento dos dados ao **mínimo necessário** e com o escopo de ser atingida a **finalidade** pretendida. Esta legislação se aplica no tratamento de **dados das pessoas naturais** e **não se aplica no tratamento de dados das pessoas jurídicas, mas todas as empresas tratam dados de pessoas naturais, ainda que de seus sócios e empregados**.

Vivemos atualmente um momento emergencial, sendo a tecnologia cada vez mais importante, incluindo métodos de inteligência artificial, drones e geolocalização, entre outros, como um grande exército no combate à Covid-19, mas não podemos esquecer da proteção de dados, dos direitos fundamentais dos titulares destes dados. A privacidade e a saúde devem interagir e dialogar, uma não pode excluir a outra. Os dados anonimizados afastam a incidência da Lei Geral de Proteção de Dados e a mesma, quando entrar em vigor, ainda nos trará dispositivos que permitem o tratamento, no combate à Covid-19, de dados pessoais e de dados pessoais sensíveis sem consentimento, com fulcro no artigo 7º, incisos III, VII e VIII e artigo 11, inciso II, letras

"b", "e" e "f", respectivamente, que estudaremos adiante, ao autorizar o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas, ao autorizar o tratamento para a proteção da vida e da incolumidade física do titular ou de terceiro e a tutela à saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde e autoridade sanitária.

A tutela dos dados da pessoa natural é indispensável em um período atual, com a rápida evolução tecnológica e a globalização, além da crescente coleta e compartilhamento sem freios dos dados pessoais. Cada vez mais as pessoas estão dependentes da tecnologia e disponibilizam seus dados pessoais de forma pública e global. As relações passaram a ser marcadas e dominadas por algoritmos de inteligência artificial (máquinas que tentam imitar a inteligência humana), *big data* (megadados ou grandes dados) e internet das coisas (que se refere à interconexão digital de objetos cotidianos com a internet). Em decorrência da rápida evolução tecnológica que vivemos no momento atual foram criados novos desafios em matéria de proteção de dados pessoais e passou-se a exigir uma maior e mais sólida proteção dos dados pessoais. Neste sentido, o Regulamento da União Europeia, trazendo a necessidade da maior proteção em seus considerandos:

> "(6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registraram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de

> uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.
>
> (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas."(4)

A Lei Geral de Proteção de Dados, como já exposto, destina-se às entidades, agentes de tratamento, as quais tratam dados pessoais e dados pessoais sensíveis das pessoas naturais, incluindo as relações de trabalho e as relações de consumo.

Esta lei não tratou de forma expressa, em seus dispositivos, as relações de trabalho, como o fez o Regulamento Geral de Proteção de Dados da União Europeia, mas também se aplica no tratamento de dados pessoais dos empregados e

---

(4) GDPR EUROPA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: <https://eu--r-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679>. Acesso em: 13 dez. 2020.

demais trabalhadores pelos empregadores, ou tomadores, os quais são os controladores desses dados e a quem cabe tomar as decisões necessárias sobre o tratamento. Quando falamos de implementação da Lei Geral de Proteção de Dados, esta não poderá ser fatiada, mas deverá abranger todos departamentos, sem exceção, onde identificados os tratamentos de dados pessoais, desde o departamento de marketing, comercial, financeiro, ao de recursos humanos, ou já teremos um GAP muito grande na implementação.

Sempre que terceirizadas as atividades de tratamento, como a gestão de folha de pagamento, a empresa responsável deverá incluir, de forma muito clara, as instruções sobre como deverão ser realizadas as atividades de tratamento, fazer uma auditoria naquela, principalmente em medidas de segurança da informação, além de incluir termos de confidencialidade (*non-disclosure agreement* – NDA) para terceiros e empregados das empresas terceirizadas.

A Lei Geral de Proteção de Dados, assim como o regulamento europeu, destina-se a proteger os dados pessoais e pessoais sensíveis de danos, no tratamento, **não apenas nos meios digitais, mas também em contratos e outros documentos escritos por meios físicos.** O artigo 5º destaca que o banco de dados consiste em um conjunto estruturado de dados em suporte eletrônico ou físico.

A Lei Geral de Proteção de Dados cria um marco legal para a proteção de informações pessoais e tem como escopo principal dar ao cidadão maior controle sobre o uso das suas informações pessoais, como já exposto anteriormente.

A legislação brasileira de proteção de dados não traz parâmetros mínimos para obrigatoriedade do registro de atividades de tratamento dos dados pessoais, estando todas empresas que tratam dados pessoais, ou dados

pessoais sensíveis, sujeitas aos registros previstos na legislação brasileira de proteção de dados, a Lei n. 13.709/2018. A Autoridade Nacional de Proteção de Dados poderá trazer parâmetros mínimos objetivos para o registro das atividades de tratamento de dados da pessoa natural.

O Considerando 13, do regulamento da União Europeia, traz uma derrogação para as organizações com menos de 250 trabalhadores, relativamente à conservação do registo de atividades. O regulamento europeu dispõe ainda, de forma expressa, no artigo 30, número 5, que a obrigação de registro não se aplica a empresas com menos de 250 pessoas, a menos que o tratamento seja suscetível de implicar risco para os direitos e liberdades do titular dos dados, não seja ocasional, ou abranja as categorias especiais de dados a que se refere o artigo 9º, número 1, ou dados pessoais relativos a condenações penais e infrações referidos no artigo 10º do regulamento europeu.(5)

É indispensável a existência de medidas técnicas e administrativas aptas a proteger e resguardar os dados pessoais e os dados pessoais sensíveis, para a proteção de direitos fundamentais de liberdade e de privacidade, de cada usuário, para evitar-se acessos não autorizados e situações acidentais ou ilícitas. Os dados pessoais deverão ser apenas tratados por pessoas que necessitem dessas informações, na realização de suas tarefas, limitando-se o tratamento ao mínimo necessário para a realização de suas finalidades. A empresa deve utilizar softwares de segurança da informação, monitoramento, criptografia, entre outros.

---

(5) GDPR EUROPA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE). Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex:32016R0679. Acesso em: 13 dez. 2020.

O uso da criptografia é um dos métodos mais eficientes para fornecer a segurança de dados, principalmente para a proteção realizada de ponta a ponta e transmitida entre as redes.

O Regulamento europeu trouxe o conceito do *privacy by design* e *privacy by default*, que foi abraçado por nossa legislação. O primeiro, privacidade desde a concepção, tem destaque na proteção do titular dos dados em toda arquitetura do negócio, em todos projetos desenvolvidos e o segundo, ou privacidade por padrão, traz a ideia de que o direito e a tecnologia devem andar juntos, que um produto ou serviço seja lançado ao público com as mais seguras configurações de privacidade. O responsável pelo tratamento de dados deverá adotar e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a concepção e por padrão.

A Lei Geral de Proteção de Dados entrou em vigor dia 18 de setembro de 2020, com a sanção da Lei n. 14.058/2020, oriunda da Medida Provisória n. 959/20, que trata da operacionalização do Benefício Emergencial. Ao editar a MP, em abril deste ano, o governo incluiu, em seu artigo 4º, um dispositivo que previa o adiamento da Lei Geral de Proteção de Dados para 3 de maio de 2021 e o qual foi retirado no dia 26 de agosto de 2020 no Senado Federal.

A Lei n. 14.010 de 2020, a qual dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado, no período da pandemia do Coronavírus (Covid-19), apenas adiou as sanções administrativas da Autoridade Nacional de Proteção de Dados para agosto de 2021, não tendo o dispositivo do PL 1.179/2020, que adiava a Lei Geral de Proteção de Dados para janeiro de 2021 sido aprovado. O texto inicial adiava a "*vacatio legis*" da Lei Geral de Proteção de Dados para 1 de janeiro de 2021, mas foi

mantida a vigência da lei para agosto de 2020 e apenas foram adiadas as sanções administrativas pela Lei n. 14.010/2020.

No Brasil, o Marco Civil da Internet, o qual foi alterado pela Lei Geral de Proteção de Dados, já nos trazia disposições sobre a proteção de dados, assim como o Código de Defesa ao Consumidor (Lei n. 8078/90) e a Lei de Cadastro Positivo (Lei n. 12.414/2011).

Capítulo 1

TRATAMENTO DE DADOS NAS RELAÇÕES DE TRABALHO

Muitas vezes, empresas acreditam estar em conformidade com a Lei Geral de Proteção de Dados, mas não adequaram os seus processos quando atinentes às relações de trabalho, principalmente no departamento de recursos humanos, onde temos uma volumetria de dados pessoais e sensíveis muito grande, sendo considerado um departamento sensível na implementação da LGPD e que inclui os empregados como titulares de dados. Lembremos que, além das sanções da Autoridade Nacional de Proteção de Dados, há possibilidade de reclamações trabalhistas de empregados e ações coletivas, sendo partes legítimas, entre outras, os sindicatos e o Ministério Público do Trabalho.

A Lei Geral de Proteção de Dados é uma lei totalmente principiológica e que também exige *compliance* trabalhista. Quando falamos de proteção de dados, especialmente nas relações de trabalho, devemos destacar que o *compliance* trabalhista consiste na cultura de adequação não apenas às regras, como aos princípios fundamentais, trazendo efetividade aos direitos humanos dos trabalhadores, no mesmo objetivo da Lei Geral de Proteção de Dados:

> "No *compliance* trabalhista devemos destacar a adequação não apenas às normas legais e regulamentares, como às normas-princípios, destacando-se

> os **princípios fundamentais previstos na Constituição Federal.**
>
> As normas-princípios são os fundamentos das normas-regras e quando uma regra colide com um princípio é na verdade não a regra que está colidindo diretamente com este, mas o princípio que a fundamenta, já que as regras conflitam enquanto os princípios colidem, não podendo haver conflito direto entre regras e princípios."(6)

Quanto à interpretação de consentimento livre, no contexto laboral, onde há desequilíbrio de poder decorrente da subordinação, defende-se que, se a ausência de consentimento vier a acarretar prejuízos relevantes reais, ou potenciais, para o empregado, o mesmo não será válido, caso seja necessário, já que não será considerado livre.

Ponto importante, muitas vezes não observado, em uma leitura rápida da Lei Geral de Proteção de Dados, nos termos do artigo 18, inciso VIII, é que o titular tem como direito: "informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa".(7)

Em determinadas situações, o tratamento poderá ser necessário para a execução de um contrato, quando se cumprem as obrigações, nos termos deste contrato, como o pagamento do empregado, quando o empregador é obrigado a tratar determinados dados pessoais, mas principalmente, temos várias normas que exigem tratamentos de dados nas relações laborais, passando o tratamento a ser uma obrigação legal ou regulatória. Caso o empregador procure invocar

(6) CARLOTO, Selma. Compliance *trabalhista*. São Paulo: LTr, 2019.
(7) BRASIL. Lei n. 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: <http://www.planalto.gov.br/cci-vil03/Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 4 jan. 2022.

o interesse legítimo, a finalidade do tratamento deverá ser legítima, devendo ser necessária, proporcional e aplicando-se a forma menos intrusiva possível.

As duas bases legitimadoras mais utilizadas em relações de emprego são as obrigações legal e regulatória, já que o Direito do Trabalho é um ramo com muita regulação e a outra a execução do contrato.

A grande empresa PwC Grécia recebeu uma multa no importe de €150Mil por violar o Regulamento Geral de Proteção de Dados da União Europeia por tratar indevidamente dados de funcionários, tendo escolhido o consentimento indevidamente, como hipótese legal de tratamento.

Interessantemente, este é o maior erro que vem se verificando em auditorias, durante e após implementação, em agentes de tratamento. É errado colocar cláusula para processar os dados do empregado com consentimento, salvo em situações pontuais em que este tem a possibilidade de autorizar ou não, sem quaisquer consequências negativas.

O empregado, assim como os clientes, pessoas naturais, como titular de seus dados pessoais, **também tem direito a receber uma política de privacidade, incluindo o compromisso da empresa, agente de tratamento, com sua privacidade, canais de coleta, finalidades de tratamento, direitos do titular, compartilhamentos, princípios aplicáveis, contato do DPO, se há transferência internacional de dados, entre outros.**

EM QUALQUER ATIVIDADE DE TRATAMENTO DE DADOS PESSOAIS, DEVER-SE-Á INFORMAR O TRATAMENTO E SUA FINALIDADE, ANTES MESMO DA COLETA, O QUE PODERÁ SER RELIZADO POR UMA POLÍTICA DE PRIVACIDADE E AVISOS.

O contrato de trabalho deverá ter uma cláusula sobre segurança da informação, mencionando a política de segurança da informação da empresa, treinamentos e termo de confidencialidade, além de uma cláusula com possibilidade de desconto, em ação regressiva, nos termos do art. 462, § 1º da CLT. (Ver modelos em anexo ao apêndice.)

O consentimento é uma das bases de tratamento, mas não é o único e no caso concreto a escolha do consentimento pela PwC, como base legitimadora, para o processamento de dados pessoais de seus funcionários não era apropriada. Estudaremos, em capítulo próprio, ao abordar o consentimento, que existe desequilíbrio de poder quando estamos diante de uma relação de emprego e esta nem sempre será a hipótese correta de tratamento. Ainda os dados dos funcionários foram processados no decorrer das atividades comerciais da empresa e os funcionários não foram informados sobre isso:

> "A PwC Grécia recebe multa de €150Mil por violar o GDPR. Órgão de proteção de dados da Grécia impôs multa de €150Mil a participação grega da PwC, "PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA", por violar o artigo 83 do GDPR.

Além disso, a Hellenic Data Protection Authority também impôs medidas corretivas à organização a serem cumpridas.

Por que a PwC foi multada?

O GDPR estabelece claramente as bases legais, sob as quais os dados pessoais podem ser processados pelos controladores. **O consentimento é uma dessas bases, mas não é o único. E a escolha do consentimento da PwC como base legal para o processamento de dados pessoais de seus funcionários não era apropriada, constatou a DPA.**