

O PAPEL DO ENCARREGADO DE DADOS NO CONTEXTO DO PROGRAMA DE *COMPLIANCE* DIGITAL

Mariana Engel Blanes Felix *

Resumo: Desde a promulgação da Lei Geral de Proteção de Dados no Brasil tem se discutido qual o real papel do Encarregado, também conhecido como DPO – *Data Protection Officer*. O objetivo do presente artigo é analisar os pontos da lei que tratam do tema e traçar um paralelo com a legislação europeia, abordando alguns outros conceitos para, ao final, indicar qual será o papel do encarregado no desafio de implementar um Programa de *Compliance* Digital.

Palavras-Chave: Lei Geral de Proteção de Dados. Encarregado. DPO. Comparativo GDPR. Funções. O papel do Encarregado no Programa de *Compliance* Digital.

1. Introdução

Muito se fala sobre a figura do Encarregado, conhecido pela *GDPR - General Data Protection Regulation*¹ como o “DPO” – *Data Protection Officer*.

Os questionamentos em torno desse tema são muitos e não se pretende, no presente artigo, esgotar todas as discussões a respeito, mas apenas trazer algumas reflexões, buscando entender ao final sobre qual é o papel do encarregado no contexto do Programa de *Compliance* Digital.

O Encarregado tem como papel principal garantir que a organização processe os dados pessoais (dos colaboradores, clientes, prestadores de serviço, fornecedores, etc.) em conformidade com as regras de proteção de dados aplicáveis.

* Advogada com mais de dezesseis anos de experiência, com forte atuação em *Compliance* e Direito Digital. É sócia em Felix Advogados. Certificada internacionalmente como DPO, pela EXIN. Citada entre as advogadas mais admiradas do RJ em Digital pela Revista Análise.

¹ Legislação Europeia de Proteção de Dados e Regulamento Geral de Proteção de Dados em tradução livre

Porém que tipo de profissional é o mais indicado para essa missão? O que fazer para alcançar o objetivo trazido pela LGPD? Quais as responsabilidades e papéis desse novo profissional? Que situações podem gerar conflitos?

Enfim, essas são algumas das indagações presentes neste artigo.

Ao longo do texto serão feitas considerações sobre a legislação brasileira, sempre traçando um paralelo com a legislação europeia e decisões proferidas pelas Autoridades Supervisoras, já que a Europa está há alguns anos à frente, considerando que a legislação sobre proteção de dados entrou em vigor por lá em 2018, existindo uma maturidade sobre o tema, bem como pelo fato de países europeus já terem enfrentado situações e dilemas que ainda não foram vivenciados no Brasil.

Após percorrer a legislação pátria e a europeia, e alguns debates já levantados e discutidos pelas Autoridades de Controle na Europa e pela Autoridade Nacional no Brasil, espera-se ter elementos suficientes para definição do papel do encarregado no contexto do Programa de *Compliance* Digital.

2. Definição do Encarregado na Lei Geral de Proteção de Dados

A Lei nº 13.709/2018, no dia 29 de maio de 2019 foi alterada, diante da aprovação da Medida Provisória nº 869/2018 pelo Senado Federal.

Dentre os pontos alterados a figura do Encarregado sofreu significativas mudanças.

No texto original, o Encarregado necessariamente deveria ser uma pessoa natural, ou seja, uma pessoa física e apenas os controladores teriam obrigação de nomeá-lo.

O artigo 41, da LGPD, indica quem deve nomear o Encarregado, mas foi logo no artigo 5º que ocorreu primeira mudança relevante, senão vejamos:

Texto original

Art. 5º

VIII – encarregado: *pessoa natural*, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

A Medida Provisória 869/2018 trouxe nova redação, mais alinhada com a realidade e necessidades que serão impostas com a vigência da lei:

Art. 5º

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

A nova redação não impõe mais a necessidade de que o Encarregado seja uma pessoa natural, permitindo a indicação de pessoas jurídicas para o desempenho dessa função.

Diante da ampliação do conceito de quem pode ser “Encarregado”, foi aberta a possibilidade da terceirização desse serviço, valendo destacar que, inclusive, não há limite territorial, o que significa dizer que poderá o Encarregado estar situado fora do território nacional, desde que preenchidos os requisitos para sua qualificação como tal.

Por fim, ampliou a figura daquele que deve nomear um Encarregado para atingir também os operadores de dados, porém não ajustou a redação do artigo 41 da LGPD, mantendo apenas o controlador como responsável pela nomeação do Encarregado.

De qualquer sorte, a despeito de não ter sido alterada a redação do artigo 41, a obrigatoriedade estende-se a todos os agentes de tratamento, inclusive as pessoas jurídicas de direito público, na forma do art. 23, III, da LGPD.

A legislação brasileira foi genérica impondo a obrigação da nomeação do Encarregado para qualquer Empresa, independente do porte.

Na legislação europeia há menção expressa de que o DPO é uma obrigação específica para Empresas com mais de 250 funcionários ou quando desenvolverem atividades previstas no artigo 37, que traz as hipóteses em que o controlador e processador deverão obrigatoriamente designar um Diretor de Proteção de Dados (DPO), equivalente ao nosso Encarregado, e são elas, quando:

a) o tratamento for efetuado por uma autoridade ou organismo público, com exceção dos órgãos jurisdicionais que atuem no exercício das suas funções;

b) as atividades principais do controlador ou do processador consistem em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidades, exigem monitoramento regular e sistemático em grande escala dos titulares dos dados ou;

c) as atividades principais do controlador ou do processador consistem no tratamento de uma grande variedade de categorias especiais de dados nos termos do Artigo 9 e dados pessoais relativos a condenações penais e infracções referidas no Artigo 10.

A GDPR trouxe os casos em que deverá ser indicado um DPO, mas não explicitou os conceitos utilizados, sendo necessário recorrer ao GT29² que emitiu orientações sobre a interpretação dos conceitos da GDPR.

Assim, o item 2.1.3 do GT29 estabeleceu que, para determinar se um tratamento de dados é efetuado em grande escala, deverá atentar-se ao:

- (i) número de titulares de dados afetados, considerando o número concreto ou em percentagem da população em causa;
- (ii) o volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento;
- (iii) a duração, ou permanência da atividade de tratamento de dados;
- (iv) o âmbito geográfico da atividade de tratamento.

Pela legislação europeia, o DPO poderá ainda ser nomeado de forma opcional, sendo certo que, se assim for feito, deverá a organização publicar os detalhes do DPO e comunicá-lo à autoridade supervisora relevante.

Já no Brasil, a Autoridade Nacional de Proteção de Dados publicou a Resolução nº 2/2022, regulamentando o tratamento jurídico para agentes de tratamento de pequeno porte, incluindo *startups* e, entre as flexibilizações, consta a dispensa da indicação do Encarregado.

Uma vez que a Empresa se enquadre nos requisitos da Resolução supracitada, não haverá necessidade de ter um Encarregado; contudo, deverá manter um canal de

² Grupo de Trabalho do artigo 29 para a Proteção de Dados (2016)

comunicação para o exercício dos direitos dos titulares.

Vale ainda ressaltar que, caso o agente de pequeno porte opte pela nomeação do *DPO*, a indicação será considerada boa prática de governança pela ANPD e isso certamente será um diferencial no mercado, demonstrando um nível de Governança frente à outras Empresas de pequeno porte ou *startups*.

A legislação brasileira não traz qualquer tipo de qualificação técnica do Encarregado. Inicialmente a Lei nº 13.709/18 havia previsto, no artigo 41, §4º³, a obrigatoriedade do Encarregado ser “detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados”.

Posteriormente, tal artigo foi vetado, não existindo mais nenhuma qualificação pré-determinada em lei.

A GDPR, por outro lado, é mais detalhista. O considerando 97 e os artigos 37.1, 37.5⁴ e 38.5 da GDPR especificam que o DPO deve ser “uma pessoa com conhecimento especializado da lei e práticas de proteção de dados”, para auxiliar o controlador ou processador, a ser “vinculado por sigilo ou confidencialidade” e “executar seus deveres e tarefas de forma independente”.

Apesar da LGPD não exigir qualquer tipo de qualificação necessária, fica clara a preocupação de que esse profissional seja multidisciplinar, que detenha vasto conhecimento sobre a Lei Geral de Proteção de Dados, bem como conhecimento sobre outras leis e regulações aplicáveis, como o Código de Defesa do Consumidor (CDC), o Marco Civil da Internet, leis trabalhistas, leis setoriais, entre outras. A LGPD não pode ser vista de forma isolada, mas ela precisa ser combinada com tantas outras que também

³Artigo 41 (...)

§ 4º Com relação ao encarregado, o qual deverá ser detentor de conhecimento jurídico-regulatório e ser apto a prestar serviços especializados em proteção de dados, além do disposto neste artigo, a autoridade regulamentará:

I - os casos em que o operador deverá indicar encarregado;

II - a indicação de um único encarregado, desde que facilitado o seu acesso, por empresas ou entidades de um mesmo grupo econômico;

III - a garantia da autonomia técnica e profissional no exercício do cargo.

4 Art. 37, item 5: O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39º.

precisam ser respeitadas. Fundamental ainda que o DPO tenha conhecimento da segurança da informação, para que ele possa exercer suas atividades tendo uma visão do todo.

Para uma Empresa estar em conformidade com a LGPD, não é possível dissociar a parte jurídica da parte de segurança da informação. O profissional que for atuar como DPO precisa, no mínimo, ter uma visão geral desses dois aspectos e cercar-se de outros profissionais que possam apoiá-lo, caso não tenha um conhecimento tão aprofundado no tema.

3. Funções esperadas do Encarregado e suas responsabilidades

Se, quando do início da vigência da LGPD, pouco se sabia sobre o trabalho e a importância dos encarregados de proteção de dados, atualmente o tema está na ordem do dia.

A função do DPO é multifacetada, devendo considerar um incidente de segurança pela ótica de todos os stakeholders (ANPD, titulares dos dados e Empresa controladora dos dados).

O artigo 41 da LGPD, §2º lista as atividades esperadas dessa função:

- I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações da autoridade nacional e adotar providências;
- III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Os itens I e II trazem, de forma objetiva, as responsabilidades do DPO; já os itens III e IV comportam um conceito mais amplo.

A 1ª atividade do DPO é tratar as solicitações do titular, o que significa dizer: dar atendimento aos direitos do Titular, que estão previstos no artigo 18⁵ da LGPD.

A 2ª atividade é realizar comunicações e providências solicitadas pela ANPD, devendo o DPO estar atento às situações que precisam ser comunicadas à ANPD, cabendo ainda à Empresa ter um plano de Resposta a Incidente, amplamente divulgado entre seus colaboradores.

A 3ª atividade do DPO é adotar as providências solicitadas pela ANPD. E o que a ANPD pode pedir?

Por exemplo, durante um processo de fiscalização ela poderá requerer:

- (i) Fornecimento de cópia de documentos, físicos ou digitais, dados e informações;
- (ii) acesso a instalações, equipamentos, sistemas e recursos tecnológicos e
- (iii) conhecimento dos sistemas utilizados e da sua atualização e rastreabilidade.

O Descumprimento poderá ser encarado como obstrução à fiscalização e dar margem à aplicação de medidas repressivas

Poderá ainda a ANPD solicitar relatório de impacto quando o tratamento tiver como fundamento seu interesse legítimo. Nesse sentido, já é recomendável que, sempre que a base legal do tratamento for legítimo interesse, a Empresa já prepare o relatório de impacto.

Dentro das atividades previstas no §2º, III, do artigo 41 da LGPD, podemos destacar a importância do DPO no processo de conscientização e aculturação da Empresa.

5 I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento

Esse movimento de mudança de cultura dentro da organização precisa ter ações coordenadas que:

- (i) Garantam a sensibilização e informação de todos os que tratem de dados pessoais;
- (ii) Assegurem o cumprimento das políticas de privacidade e proteção de dados;
- (iii) Promovam boas práticas para a proteção de dados;

O Encarregado tem um papel fundamental na consolidação do conhecimento da Lei, Políticas e normas da Empresa. Ele precisará treinar replicadores nos diversos departamentos, pessoas que possam atuar como sua extensão, auxiliando na identificação das falhas e riscos, acionando o DPO quando necessário.

Para isso o Encarregado deverá determinar conteúdo, formato, público-alvo e demais detalhes do Plano de Treinamento e Comunicação em Proteção de Dados, levando em consideração as necessidades e os riscos do negócio.

Outras atividades do DPO são:

- (i) Controlar e regular a conformidade da LGPD;
- (ii) Recolher informação para identificar atividades de tratamento;
- (iii) Controlar o cumprimento de contratos escritos;
- (iv) Realizar a avaliação na exposição aos riscos de violações de privacidade e adotar ações para mitigá-los, dentre tantas outras necessárias para manter a Empresa em conformidade com a Lei Geral de Proteção de Dados.

4. Possíveis Conflitos no desempenho da função

O DPO deve exercer suas atividades com máxima independência e ser sempre envolvido de forma adequada, em tempo hábil, apoiado por uma equipe multidisciplinar que reúna competências nas mais diversas áreas (financeira, recursos humanos, tecnológica, marketing, arquivo, entre outras), cabendo à Empresa prover os recursos necessários para o desempenho das suas funções.

O DPO não deverá receber instruções sobre o desempenho das suas funções e deve se reportar à alta administração

É recomendável que ele tenha orçamento próprio e tenha o poder de auditar e questionar sobre o processamento de dados nas diversas áreas da Empresa.

A sua remuneração não deve ser atrelada aos ganhos da Empresa e também não pode haver Conflito de Interesses entre os deveres do indivíduo, na qualidade de DPO e seus outros deveres, se acumular outros cargos.

Sobre esse ponto, as Autoridades de Controle, que são o equivalente à nossa ANPD na Europa, já se posicionaram, merecendo destaque as decisões a seguir comentadas.

Em 2016 a Autoridade de Proteção de Dados da Baviera para o Setor Privado ('BayLDA') impôs multa a uma Empresa porque o DPO desta tinha um conflito de interesses. Segundo a Autoridade de Controle, o conflito de interesses existia porque o DPO também ocupava o cargo de gerente de TI na mesma Empresa. Manter uma posição diretamente ligada às atividades de processamento de dados e ser DPO geralmente traz a incompatibilidade das tarefas, posto que ele mesmo deveria fazer uma auto-inspeção do seu trabalho.

Nesse julgado foram trazidas outras hipóteses de conflito, sobre as quais vale a pena uma reflexão:

- (i) Prestador de serviço de TI de maneira significativa que também forneça os serviços do DPO externo; e
- (ii) conflitos de interesse da família, como quando o DPO é relacionado por sangue ou casamento ao diretor administrativo.

Já em 28 de abril de 2020, a Câmara de Litígios da Autoridade Belga de Proteção de Dados impôs uma multa de € 50.000 a uma Empresa por não conformidade com a GDPR, devido à nomeação de um oficial de proteção de dados (“DPO”).

Na sua decisão, a Câmara de Litígios da Autoridade de Controle Belga argumentou que, ao nomear o Chefe do departamento de Compliance, Gerenciamento de Riscos e Auditoria como DPO, a Empresa não cumpriu sua obrigação de garantir que o DPO estivesse livre de conflito de interesse.

O principal argumento levantado pela autoridade Belga foi que, em razão da combinação de funções, não haveria supervisão independente do DPO referente às atividades de processamento de dados, que ocorrem no contexto dos departamentos de conformidade, gerenciamento de riscos e auditoria.

Devido à sua dupla função, o DPO pode não ser capaz de fornecer garantias suficientes aos funcionários envolvidos, em termos de confidencialidade e sigilo.

Esse aspecto da autonomia é muito importante para que o DPO cumpra o seu munus, pois se ele está subordinado a alguma gerência, fica difícil apresentar as falhas daquele departamento, comprometendo toda a sua atuação.

Outro ponto relevante é que, com a cumulação de atividades, muitas vezes a Empresa não fornece estrutura necessária, faltando tempo ao profissional para o exercício da função de DPO, já que este acaba por priorizar a sua atividade primária, da qual é cobrado pela diretoria ou gerência.

5. Considerações finais

Diante do exposto, é fundamental que o Encarregado tenha conhecimentos jurídicos e de segurança da informação, que possa acompanhar e envolver-se nos principais fluxos de processos que exponham dados pessoais dentro da Empresa, bem como auxiliar diretamente no desenvolvimento de novos produtos e serviços, de forma que possa supervisionar as práticas de tratamento de dados.

Para isso, será de suma importância que o Encarregado desempenhe suas funções com autonomia e imparcialidade dentro das organizações, podendo ele interferir nos processos internos e sugerir mudanças e adequações, visando sempre a manter o *compliance* com a Lei Geral de Proteção de Dados.

REFERÊNCIAS:

BRASIL. Câmara dos Deputados. Lei 13.709. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 04 julho 2020.

BRASIL. Câmara dos Deputados. Medida Provisória 869. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm>. Acesso em: 04 julho 2020.

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. Regulamento Geral sobre a Proteção de Dados. Disponível em: Acesso em: 04 julho 2020.

Comissão Europeia (2010). A comprehensive approach on personal data protection in the European Union COM (2010) 609 final. Jornal Oficial da União Europeia N.º C121, 19.04.2011.

^{3/4} Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (2016). Orientações sobre os encarregados da proteção de dados (EDP) WP243rev.01. Disponível nos portais: https://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=612048; <https://www.autoriteprotectiondonnees.be/citoyen>