

ÍNDICE

PREFÁCIO	17
NOTA INTRODUTÓRIA	21
SÍMBOLOS USADOS	25
GLOSSÁRIO	27
SIGLAS E ACRÓNIMOS	35
PARTE I O PAPEL DO DEPARTAMENTO DE RECURSOS HUMANOS NA CONFORMIDADE COM O RGPD	37
PARTE II COMO ESTÁ ORGANIZADO O GUIA PRÁTICO?	45
PARTE III GUIA PRÁTICO PARA A CONFORMIDADE COM O RGPD	67
III.AT. Aspectos transversais da conformidade com o RGPD	67
III.AT.1. Exercício de direitos por parte dos titulares de dados pessoais	67
III.AT.1.1. Enquadramento jurídico	68
Que direitos de proteção de dados pessoais podem ser exercidos por um trabalhador junto do seu empregador?	68
Direito à informação: prestação de informação aos titulares dos dados (trabalhadores)	69
Qual o dever do empregador, enquanto responsável pelo tratamento, face a um pedido de exercício de direitos?	70
III.AT.1.2. Auditoria e recomendações para a conformidade – RGPD	71
Requisitos ISO 27001 e RGPD	71
Objetivos de controlo	72

Avaliação de riscos	73
Sugestão de medidas de controlo a implementar	74
III.AT.2. Incidentes de segurança da informação e de proteção de dados pessoais, e regime sancionatório	77
III.AT.2.1. Enquadramento jurídico	77
Regime contraordenacional previsto na Lei de Execução	80
III.AT.2.2. Auditoria e recomendações para a conformidade – RGPD	82
Requisitos ISO 27001 e RGPD	82
Objetivos de controlo	82
Avaliação de riscos	83
Sugestão de medidas de controlo a implementar	84
III.AT.3. Nomeação e funções do encarregado da proteção de dados	87
III.AT.3.1. Enquadramento jurídico	87
Designação do EPD	87
Competências e conhecimentos especializados do EPD	89
Modelo de comunicação com o EPD	91
Funções do EPD	92
Responsabilidade civil profissional do EPD	94
III.AT.3.2. Auditoria e recomendações para a conformidade – RGPD	95
Requisitos ISO 27001 e RGPD	95
Objetivos de controlo	95
Avaliação de riscos	96
Sugestão de medidas de controlo a implementar	97
III.AT.4. Avaliação de impacto para a proteção de dados pessoais (AIPD)	99
III.AT.4.1. Enquadramento jurídico	99
Realização de uma AIPD	100
Realização de uma consulta prévia à autoridade de controlo	100
III.AT.4.2. Auditoria e recomendações para a conformidade – RGPD	102
Requisitos ISO 27001 e RGPD	102
Objetivos de controlo	103
Avaliação de Riscos	103
Sugestão de medidas de controlo a implementar	104
III.AT.5. Subcontratação e responsabilidades – RGPD	105
III.AT.5.1. Enquadramento jurídico	106
A figura do subcontratante para o RGPD	106
Acordos de subcontratação no âmbito da relação laboral	107
Cláusulas Contratuais-Tipo (CCT) para regulação de subcontratantes dentro do Espaço Económico Europeu	109

Cláusulas Contratuais-Tipo (CCT) para transferência de dados pessoais para países terceiros	110
Dever de informar os trabalhadores dos subcontratantes utilizados no âmbito da relação laboral	112
Direito de indemnização e responsabilidade civil do responsável pelo tratamento e do subcontratante	112
III.AT.5.2. Auditoria e recomendações para a conformidade – RGPD	113
Requisitos ISO 27001 e RGPD	113
Objetivos de controlo	113
Avaliação de riscos	114
Sugestão de medidas de controlo a implementar	115
III.AT.6. A utilização de algoritmos na gestão dos recursos humanos	117
O conceito de “algoritmo”	117
Vantagens decorrentes da utilização dos algoritmos no âmbito da relação laboral	118
O “novo petróleo” na gestão de RH	119
Riscos associados à utilização dos Algoritmos	120
Empregadores nas malhas dos algoritmos	125
III.AT.6.1. Enquadramento jurídico	126
Da fundamentação para a utilização de algoritmos no âmbito da relação laboral	126
Do dever de informação	126
Do dever de transparência	127
Da utilização de algoritmos e dos requisitos para a conformidade com o RGPD	129
III.AT.6.2. Auditoria e recomendações para a conformidade – RGPD	131
Requisitos ISO 27001 e RGPD	131
Objetivos de controlo	132
Avaliação de riscos	133
Sugestão de medidas de controlo a implementar	135
III.RH. Conformidade com o RGPD nos tratamentos de dados dos RH	137
... até à formalização do contrato (diligências pré-contratuais)	137
III.RH.1. Seleção e recrutamento/receção e tratamento de <i>curricula vitae</i>	137
III.RH.1.1. Enquadramento jurídico	137
O que podemos perguntar a um candidato a emprego? Que documentos/certificados podemos pedir? Podemos armazenar esses dados? Até quando?	137

Que interesses poderão então justificar a compressão do direito à privacidade dos candidatos a emprego?	138
<i>Background checks</i>	139
Recrutamento <i>online</i>	140
Recrutamento eletrónico/Definição de perfis	141
Serviços de apoio à distância e <i>call centres</i>	142
Podemos armazenar os dados referentes a um processo de recrutamento?	
Até quando?	142
Elementos a fazer constar de um modelo de declaração informativa relativa à recolha e tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento	145
Finalidades do tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento	145
Fundamentos para o tratamento de dados pessoais no âmbito de um processo de seleção e recrutamento	145
Categorias de dados pessoais do trabalhador a tratar	146
Transferências de dados para terceiros	146
Os direitos do candidato a emprego	147
Período de retenção	147
Medidas de Segurança	147
Contactos	147
Direito a apresentar queixa perante a autoridade de controlo	147
III.RH.1.2. Auditoria e recomendações para a conformidade – RGPD	148
Receção e tratamento de <i>curricula vitae</i>	148
Requisitos ISO 27001 e RGPD	148
Objetivos de controlo	148
Avaliação de riscos	150
Sugestão de medidas de controlo a implementar	150
Processo de seleção e recrutamento	152
Requisitos ISO 27001 e RGPD	152
Objetivos de controlo	152
Avaliação de riscos	153
Sugestão de medidas de controlo a implementar	153
III.RH.2. Recolha e tratamento de dados pessoais com vista à contratação laboral	154
III.RH.2.1. Enquadramento jurídico	154
Das finalidades para o tratamento de dados pessoais dos trabalhadores	154
Fundamentos para o tratamento de dados pessoais no âmbito da relação laboral	156
O consentimento dos trabalhadores	157

III.RH.2.2. Auditoria e recomendações para a conformidade – RGPD	159
Requisitos ISO 27001 e RGPD	159
Objetivos de controlo	160
Avaliação de riscos	160
Sugestão de medidas de controlo a implementar	161
III.RH.3. Contratação (diligências para)	161
III.RH.3.1. Enquadramento jurídico	161
Finalidade do tratamento e fundamento jurídico específico	162
Categorias de dados a tratar no âmbito da relação de trabalho	163
Dados pessoais de terceiros	165
Utilização de subcontratantes / Dever de informação a prestar aos trabalhadores	166
III.RH.3.2. Auditoria e recomendações para a conformidade – RGPD	166
Requisitos ISO 27001 e RGPD	166
Objetivos de controlo	167
Avaliação de riscos	167
Sugestão de medidas de controlo a implementar	168
... durante a relação laboral	170
III.RH.4. Sensibilização e compromisso com regulamentos e regras de conduta	170
III.RH.4.1. Enquadramento jurídico	170
Normas internas: regulamentos e regras de conduta	170
III.RH.4.2. Auditoria e recomendações para a conformidade – RGPD	171
Requisitos ISO 27001 e RGPD	171
Objetivos de controlo	172
Avaliação de riscos	172
Sugestão de medidas de controlo a implementar	173
III.RH.5. Atribuição de acessos físicos e acessos aos sistemas informáticos	175
III.RH.5.1. Enquadramento jurídico	175
Fundamento	175
Enquadramento legal	176
Controlo do <i>email</i> dos trabalhadores	176
Monitorização do uso da internet	177
Acesso remoto ao computador do trabalhador	177
Controlo de dados de comunicações telefónicas e de tráfego	178
III.RH.5.2. Auditoria e recomendações para a conformidade – RGPD	178
Requisitos ISO 27001 e RGPD	178
Objetivos de controlo	179

Avaliação de riscos	179
Sugestão de medidas de controlo a implementar	180
III.RH.6. Atribuição de equipamentos informáticos e dispositivos eletrónicos	182
III.RH.6.1. Enquadramento jurídico	182
III.RH.6.2. Auditoria e recomendações para a conformidade – RGPD	183
Requisitos ISO 27001 e RGPD	183
Objetivos de controlo	183
Avaliação de riscos	184
Sugestão de medidas de controlo a implementar	184
III.RH.7. Gestão de horários, turnos e escalas	185
III.RH.7.1. Enquadramento jurídico	185
III.RH.7.2. Auditoria e recomendações para a conformidade – RGPD	187
Requisitos ISO 27001 e RGPD	187
Objetivos de controlo	187
Avaliação de riscos	188
Sugestão de medidas de controlo a implementar	188
III.RH.8. Gestão de férias, ausências e justificação	189
III.RH.8.1. Enquadramento jurídico	189
Fundamento de licitude	189
Faltas e sua justificação	190
III.RH.8.2. Auditoria e recomendações para a conformidade – RGPD	192
Requisitos ISO 27001 e RGPD	192
Objetivos de controlo	192
Avaliação de riscos	192
Sugestão de medidas de controlo a implementar	193
III.RH.9. Segurança, higiene e saúde no trabalho	194
III.RH.9.1. Enquadramento jurídico	194
Tratamento de dados pessoais para efeitos de segurança e saúde no trabalho	194
Controlo de alcoolemia e de consumo de estupefacientes	195
Vacinação de trabalhadores	197
Ação dos responsáveis pela segurança, higiene e saúde no trabalho	199
III.RH.9.2. Auditoria e recomendações para a conformidade – RGPD	200
Requisitos ISO 27001 e RGPD	200
Objetivos de controlo	200
Avaliação de riscos	201
Sugestão de medidas de controlo a implementar	201
III.RH.10. Publicações de reporte obrigatório	202
III.RH.10.1. Enquadramento jurídico	202

III.RH.10.2. Auditoria e recomendações para a conformidade – RGPD	204
Requisitos ISO 27001 e RGPD	204
Objetivos de controlo	204
Avaliação de riscos	204
Sugestão de medidas de controlo a implementar	205
III.RH.11. Processamento salarial	206
III.RH.11.1. Enquadramento jurídico – Código do Trabalho	206
Fundamento de licitude	206
Utilização de um subcontratante para o processamento salarial	207
III.RH.11.2. Auditoria e recomendações para a conformidade – RGPD/ Código do Trabalho	209
Requisitos ISO 27001 e RGPD	209
Objetivos de controlo	209
Avaliação de riscos	209
Sugestão de medidas de controlo a implementar	210
III.RH.12. Seguros para trabalhadores	212
III.RH.12.1. Enquadramento jurídico	212
III.RH.12.2. Auditoria e recomendações para a conformidade – RGPD	213
Requisitos ISO 27001 e RGPD	213
Objetivos de controlo	213
Avaliação de riscos	214
Sugestão de medidas de controlo a implementar	214
III.RH.13. Divulgação dos contactos de trabalhadores a terceiros	215
Qual a legitimidade do empregador, e dos seus trabalhadores, para divulgar contactos, pessoais e profissionais, dos trabalhadores junto de terceiros?	216
III.RH.13.1. Enquadramento jurídico	216
III.RH.13.2. Auditoria e recomendações para a conformidade – RGPD	217
Requisitos ISO 27001 e RGPD	217
Objetivos de controlo	217
Avaliação de riscos	217
Sugestão de medidas de controlo a implementar	217
III.RH.14. Atribuição de veículo automóvel, equipamentos de identificação e georreferenciação	220
III.RH.14.1. Enquadramento jurídico	221
Necessidade de realizar uma avaliação de impacto sobre a proteção de dados pessoais (AIPD)	222
Pedido de parecer à comissão de trabalhadores	223
Celebração de acordo de subcontratação do tratamento de dados pessoais	224
Prestação de informação aos titulares dos dados (trabalhadores)	224
Atualização do registo das atividades de tratamento	224

III.RH.14.2. Auditoria e recomendações para a conformidade – RGPD	225
Requisitos ISO 27001 e RGPD	225
Objetivos de controlo	226
Avaliação de riscos	226
Sugestão de medidas de controlo a implementar	227
III.RH.15. Arquivo da ficha individual do trabalhador	228
III.RH.15.1. Enquadramento jurídico	229
III.RH.15.2. Auditoria e recomendações para a conformidade – RGPD	230
Requisitos ISO 27001 e RGPD	230
Objetivos de controlo	231
Avaliação de riscos	232
Sugestão de medidas de controlo a implementar	232
III.RH.16. Recolha, tratamento e divulgação da imagem de trabalhadores	234
III.RH.16.1. Enquadramento jurídico	234
Minuta de declaração/Pedido de consentimento	234
III.RH.16.2. Auditoria e recomendações para a conformidade – RGPD	236
Requisitos ISO 27001 e RGPD	236
Objetivos de controlo	236
Avaliação de riscos	237
Sugestão de medidas de controlo a implementar	237
III.RH.17. Videovigilância (CCTV)	238
III.RH.17.1. Enquadramento jurídico e Código do Trabalho	239
Finalidades legalmente admissíveis	240
Dever de informação aos trabalhadores (e a outros titulares de dados)	241
Obrigações a cumprir aquando da instalação de um sistema de videovigilância	242
Locais objeto de videovigilância	242
Processo de instalação de dispositivo de videovigilância	243
Pedido de autorização à CNPD?	244
Pedido de parecer à comissão de trabalhadores	244
A utilização das imagens recolhidas: usos permitidos	245
Utilização de imagens de videovigilância para fins disciplinares	245
III.RH.17.2. Auditoria e recomendações para a conformidade – RGPD	247
Requisitos ISO 27001 e RGPD	247
Objetivos de controlo	247
Avaliação de riscos	248
Sugestão de medidas de controlo a implementar	249
III.RH.18. Utilização de dados biométricos de trabalhadores no âmbito da relação laboral	251

III.RH.18.1. Enquadramento jurídico	251
Processo de instalação/utilização de dispositivos de biometria	253
Abolição do pedido de notificação à CNPD	253
Dever de informação em matéria de dados biométricos	254
Pedido de parecer à comissão de trabalhadores	255
III.RH.18.2. Auditoria e recomendações para a conformidade – RGPD	256
Requisitos ISO 27001 e RGPD	256
Objetivos de controlo	256
Avaliação de riscos	257
Sugestão de medidas de controlo a implementar	258
III.RH.19. A gravação de chamadas telefónicas e o seu impacto nas relações laborais	259
III.RH.19.1. Enquadramento jurídico	259
As chamadas telefónicas que realizamos no local de trabalho podem ser gravadas?	259
Chamadas pessoais <i>versus</i> chamadas profissionais	260
Qual o enquadramento legal aplicável?	260
A validade da Deliberação n.º 629/2010 da Comissão Nacional de Proteção de Dados	261
Tratamento de dados pessoais decorrentes da gravação de chamadas, efetuada no âmbito da monitorização da qualidade do atendimento	261
Fundamentos para a recolha de dados dos trabalhadores para efeitos de gravação de chamadas	263
Tratamento de dados pessoais decorrente da gravação de chamadas efetuada no âmbito de uma relação contratual	265
Tratamento de dados pessoais decorrentes da gravação de chamadas efetuada no âmbito de uma situação de emergência	266
Prazo de conservação das gravações	267
Subcontratante	267
III.RH.19.2. Auditoria e recomendações para a conformidade – RGPD	268
Requisitos ISO 27001 e RGPD	268
Objetivos de controlo	268
Avaliação de riscos	269
Sugestão de medidas de controlo a implementar	270
III.RH.20. Teletrabalho	270
III.RH.20.1. Enquadramento jurídico	271
Conceito	271
Nem todo o teletrabalho é igual	272
Instrumentos de trabalho	272

Controlo de assiduidade e da pontualidade	274
Outros controlos à distância	275
Direito a desligar	275
III.RH.20.2. Auditoria e recomendações para a conformidade – RGPD	277
Requisitos ISO 27001 e RGPD	277
Objetivos de controlo	277
Avaliação de riscos	278
Sugestão de medidas de controlo a implementar	281
III.RH.21. Monitorização da temperatura corporal dos trabalhadores	284
III.RH.21.1. Enquadramento jurídico	285
Posição da CNPD	285
Opção legislativa	285
Temperatura normal?	286
Dever de informação aos trabalhadores	287
Legitimidade para proceder à monitorização da temperatura dos trabalhadores	287
III.RH.21.2. Auditoria e recomendações para a conformidade – RGPD	288
Requisitos ISO 27001 e RGPD	288
Objetivos de controlo	289
Avaliação de riscos	289
Sugestão de medidas de controlo a implementar	290
III.RH.22. Sanções disciplinares	291
III.RH.22.1. Enquadramento jurídico	292
III.RH.22.2. Auditoria e recomendações para a conformidade – RGPD	293
Requisitos ISO 27001 e RGPD	293
Objetivos de controlo	293
Avaliação de riscos	294
Sugestão de medidas de controlo a implementar	294
III.RH.23. Tratamento de dados de condenações penais e de diversas infrações	296
III.RH.23.1. Enquadramento jurídico	297
III.RH.23.2. Auditoria e recomendações para a conformidade – RGPD	299
Requisitos ISO 27001 e RGPD	299
Objetivos de controlo	300
Avaliação de riscos	300
Sugestão de medidas de controlo a implementar	301
III.RH.24. Tratamento de dados de menores	302
III.RH.24.1. Enquadramento jurídico	302
Tratamento de dados de terceiros – descendentes dos trabalhadores	303
Contactos de terceiros para situações de emergência	304

III.RH.24.2. Auditoria e recomendações para a conformidade – RGPD	305
Requisitos ISO 27001 e RGPD	305
Objetivos de controlo	305
Avaliação de riscos	306
Sugestão de medidas de controlo a implementar	306
III.RH.25. Whistleblowing – A proteção (dos trabalhadores) denunciantes de infrações ao direito da União e o combate ao assédio no local de trabalho	308
III.RH.25.1. Enquadramento jurídico	308
Denunciantes protegidos = trabalhadores protegidos	310
Novas obrigações legais para as organizações	311
Formas de apresentação das denúncias	312
Fundamentos jurídicos aplicáveis	312
Pedido de parecer à comissão de trabalhadores	313
Realização de uma avaliação de impacto sobre a proteção de dados (AIPD)	313
Prazos de conservação	314
Regime sancionatório	314
III.RH.25.2. Auditoria e recomendações para a conformidade – RGPD	315
Requisitos ISO 27001 e RGPD	315
Objetivos de controlo	315
Avaliação de riscos	316
Sugestão de medidas de controlo a implementar	317
III.RH.26. Alteração de funções e de responsabilidades	319
III.RH.26.1. Enquadramento jurídico	320
III.RH.26.2. Auditoria e recomendações para a conformidade – RGPD	321
Requisitos ISO 27001 e RGPD	321
Objetivos de controlo	321
Avaliação de riscos	322
Sugestão de medidas de controlo a implementar	322
Diligências com vista à cessação contratual	324
III.RH.27. Cessação do contrato de trabalho	324
III.RH.27.1. Enquadramento jurídico	324
III.RH.27.2. Auditoria e recomendações para a conformidade – RGPD	325
Requisitos ISO 27001 e RGPD	325
Objetivos de controlo	326
Avaliação de riscos	326
Sugestão de medidas de controlo a implementar	327
III.RH.28. Entrega de bens e cessação de acessos físicos e lógicos	328
III.RH.28.1. Enquadramento jurídico	328

Entrega das ferramentas de trabalho	328
Conteúdo da caixa de correio eletrónico (<i>email</i>)	328
III.RH.28.2. Auditoria e recomendações para a conformidade – RGPD	329
Requisitos ISO 27001 e RGPD	329
Objetivos de controlo	330
Avaliação de riscos	330
Sugestão de medidas de controlo a implementar	331
III.RH.29. Retenção e destruição dos dados	332
III.RH.29.1. Enquadramento jurídico	332
Princípios a ter conta no tocante à conservação dos dados	334
Direito ao apagamento – direito diferido no tempo	336
Alternativas ao apagamento dos dados	337
Prazos de conservação	337
III.RH.29.2. Auditoria e recomendações para a conformidade – RGPD	338
Requisitos ISO 27001 e RGPD	338
Objetivos de controlo	338
Avaliação de riscos	339
Sugestão de medidas de controlo a implementar	340
BIBLIOGRAFIA	343

PREFÁCIO

1. Uma boa parte dos portugueses já ouviu seguramente falar do escândalo Facebook – Cambridge Analytica, o qual provou a relevância da utilização na vida política de grandes volumes de dados pessoais. Foi assim no referendo sobre o Brexit, foi assim também nas últimas eleições norte-americanas. No fundo, em termos gerais, o que sucedeu foi isto: com o acesso a uma quantidade significativa de informação sobre utilizadores de *sites* ou redes sociais, manipularam-se campanhas políticas, usando e abusando de dados pessoais dos cidadãos, à sua revelia, sem o seu consentimento e mesmo sem o seu conhecimento. Algo de absolutamente indigno e ilegítimo.

Há duas dezenas de anos, esta realidade era inimaginável. Para a generalidade dos cidadãos, qualquer cenário desta natureza seria visto, então, como um mero exercício de ficção científica. Interessante do ponto de vista da especulação, inverosímil na perspetiva da realidade do dia a dia.

Só que o tempo mudou, a dinâmica da vida em sociedade acelerou, a investigação atingiu proporções nunca vistas e, dessa forma, a tecnologia alterou radicalmente a nossa vida. Hoje, o avanço tecnológico é brutal. A internet modificou, de alto a baixo, os nossos comportamentos tradicionais. Os *sites*, as redes sociais, os blogues, a informação *online* são exemplos de mudanças que tornaram a nossa vida mais ágil, mais completa, mais preenchida e com mais oportunidades. Tudo isto é positivo. Mas tudo isto tem também o seu lado perverso e perigoso – e um desses lados é o da potencial violação dos dados pessoais dos cidadãos, que o mesmo é dizer o afronto à sua legítima privacidade.

2. Mesmo com toda a modernidade dos nossos dias – ou justamente por causa dela – o direito e dever à proteção dos nossos dados é cada vez mais importante e essencial. E não é apenas no domínio da vida política. É em qualquer outro patamar do nosso quotidiano. Afinal, do que se trata é de salvaguardar um direito fundamental do cidadão, é de não permitir a violação da intimidade de quem quer que seja, é de não pactuar com a ideia do vale tudo, sem regras, sem princípios, sem escrúpulos.

Uma tarefa desta natureza, sendo essencial no plano dos princípios, não é fácil de concretizar na prática. Desde logo porque, para ser minimamente eficaz, tem de ter uma natureza transnacional. Também aqui, ou sobretudo aqui, no domínio tecnológico, o tempo do Estado-Nação tradicional acabou, dando lugar ao primado da aldeia global e do mundo cada vez mais desprovido de barreiras ou fronteiras.

É nestas ocasiões que a União Europeia é um projeto arrojado e fundamental. Não apenas por ser uma União de Estados e de povos. Mas por ser, além disso, uma União de valores, princípios e interesses essenciais ao futuro da comunidade. Cumprindo o seu desiderato, a União Europeia fez aprovar em 2016 o chamado Regulamento Geral sobre a Proteção de Dados, aquele que é considerado o regime mais avançado, mais moderno e mais rigoroso que se conhece na defesa dos cidadãos contra os efeitos anómalos da tecnologia, na proteção dos dados individuais de cada um, na afirmação de uma vivência em sociedade mais segura e mais madura. E Portugal, seguindo o seu exemplo, aprovou em 2019 o caminho a seguir, através da aprovação da Lei n.º 58/2019, de 8 de agosto. Um momento essencial nas nossas vidas e na vivência em sociedade.

3. Este livro é disso mesmo que trata – de explicar a realidade legal da proteção de dados pessoais no domínio das empresas, de informar os cidadãos sobre esta realidade na vertente laboral, de esclarecer empregadores e empregados, de criar um ágil instrumento de trabalho para gestores, diretores e trabalhadores.

Com duas vantagens:

- Primeiro, este é um livro escrito por quem sabe, por quem tem experiência, por quem lida com estas questões, por quem é exemplo e referência nesta área. Simão de Sant’Ana, meu colega de escritório, é um advogado competente, experiente, dedicado e conhecedor. Mormente nesta área, Vitorino Gouveia, mestre em

Engenharia Informática, é, por sua vez, um técnico experiente e qualificado. Ambos são uma mais-valia nesta temática.

- Depois, este livro não é um compêndio de generalidades ou abstrações. Muito menos uma compilação de diagnósticos. Pelo contrário, é um apoio muito prático e uma ajuda muito objetiva. Perante um problema concreto na aplicação dentro das empresas da legislação sobre dados pessoais, este livro responde, informa, esclarece e ajuda a resolver. É objetivamente um guia prático de grande significado e importância. Uma ferramenta de apoio para gestores, diretores ou trabalhadores.

Porque todos, nesta fase capital de adaptação a uma nova realidade, merecem e precisam de apoio. Porque esta mudança essencial nem sempre é fácil de interiorizar e aplicar. Porque o futuro requer que sejamos capazes de potenciar o desenvolvimento tecnológico sem descurar a proteção dos nossos dados pessoais, que o mesmo é dizer, sem abdicar da nossa identidade e da dignidade de cidadãos livres que nos orgulhamos de ser.

LUÍS MARQUES MENDES

NOTA INTRODUTÓRIA

A entrada em vigor do Regulamento Geral sobre a Proteção de Dados¹ (RGPD) e a publicação da Lei n.º 58/2019 de 8 de agosto (a “Lei de Execução”)² trouxeram a temática da proteção dos dados pessoais para o quotidiano das empresas.

Os elevados valores das coimas previstas no RGPD vieram a suscitar o interesse dos *media* sobre o assunto. Agora, mais do que nunca, a temática dos dados parece ter conquistado preeminência em todo o tipo de publicações, incluindo os noticiários. Outrora quase exclusivamente restrita ao meio académico, tornou-se matéria do nosso dia a dia.

Mas porque terão aqueles diplomas legais suscitado tal interesse? Serão só as multas? Não o cremos, pois não é a primeira vez que um diploma legal estabelece um regime sancionatório gravoso, sem que isso alguma vez tenha gerado grande alarido.

Afinal, o RGPD foi apenas o gatilho que chamou a atenção para novos problemas criados pelo novo mundo tecnológico em que vivemos. De facto, a proteção de dados deixou de ser apenas um princípio constitucional de cariz distante. Agora, interage diretamente com todos.

Mas porquê? Bem, em poucas palavras, porque a tecnologia mudou tudo à nossa volta – mudou a forma como vivemos.

¹ Regulamento (UE) 2016/679 do Parlamento e do Conselho Europeus, 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 (3).

² A qual assegura a execução na ordem jurídica nacional do RGPD.

Num passado pouco distante, os miúdos pediam à mãe para fazer aquele bolo especial – hoje pedem um *uber eats* e, 30 minutos mais tarde, se tudo correr bem, o desejo é satisfeito. Independentemente de todas as suas potenciais consequências sociológicas, este novo tipo de comportamento exige que se recolham os dados de um cartão de crédito, os quais são tratados e arquivados por uma entidade prestadora de serviços de entregas, com sede algures no mundo. Além disso, a empresa de entregas, bem como o próprio prestador do serviço de restauração, ficam a saber o que aquela família gosta de consumir, em que dias, a que horas, com que frequência, onde mora, etc. Se multiplicarmos isto por milhões de utilizadores espalhados por todo o mundo, temos uma base de dados mundial sobre hábitos de consumo, a qual valerá muitos milhões de euros.

O mesmo se diga em relação ao Facebook, ao Google/Gmail ou ao YouTube. Já parou para pensar porque é que estas e outras empresas tecnológicas, avaliadas em biliões de dólares, lhe prestam serviços gratuitos? Desengane-se, pois a resposta não é a mera venda de publicidade. Tal como Yuval Noah Harari – o historiador israelita autor de *Homo Sapiens*, disse à revista *Time*: “Dão-lhe redes sociais gratuitas e vídeos cómicos sobre gatos. Em troca, você renuncia ao seu bem mais precioso, os seus dados pessoais.”³

Mas a revolução tecnológica foi mais longe e infiltrou-se no mundo do trabalho: longe vão os dias em que os tempos de trabalho se registavam manualmente nos livros de ponto. Hoje, passamos o dedo, e os sistemas biométricos do empregador acusam a nossa chegada às instalações da empresa; mal passamos a entrada, as câmaras de videovigilância captam a nossa imagem; ligamos o computador e, através do sistema informático do empregador, enviamos *emails*, uns profissionais, outros nem tanto; não satisfeitos, navegamos a internet no computador que colocaram em cima da nossa secretária, acedemos às notícias que mais nos interessam, acedemos ao *homebanking*, fazemos compras, etc. Tudo com as ferramentas informáticas do empregador – as quais, diga-se, têm a capacidade de monitorizar o que fazemos, como fazemos e quando fazemos, minuto a minuto.

Ora, esta potencial invasão de privacidade ao mundo dos trabalhadores só é acautelada graças a diplomas legais como o RGPD e à demais legislação nacional relativa ao trabalho e à proteção de dados pessoais.

³ Tradução nossa. In revista *Time*, 27 de fevereiro a 6 de março de 2017, p. 92, entrevista de Nate Hopper: “You get free social media services, and you get free funny cat videos. In exchange, you give up the most valuable asset you have, which is your personal data.”

Porém, tais diplomas não detalham com suficiência a disciplina que deve governar a privacidade dos trabalhadores no seio das empresas. Aqui, são necessários regulamentos internos e manuais de boas práticas capazes de defender os interesses de ambas as partes – pois, acima de tudo, são as empresas quem mais precisa de se proteger contra os eventuais abusos perpetrados quer por terceiros, quer pelos seus próprios trabalhadores.

Se, por um lado, a produtividade dos trabalhadores e os direitos de propriedade industrial das empresas não podem servir de justificação para uma monitorização total dos trabalhadores – que é, aliás, proibida por lei –, muitas grandes e pequenas empresas já foram apanhadas desprevenidas e viram os seus segredos transmitidos à concorrência, sem saberem como reagir.

É verdade que não podemos impedir a cada vez mais invasiva e abrangente tecnologia que todos os dias aterra no mundo do trabalho, porque ela é essencial à persecução dos interesses das empresas. Logo, há que criar mecanismos que permitam às empresas tirar partido da tecnologia em cumprimento da lei e, concludentemente, evitando ataques cibernautas, fugas de informação confidencial, perdas acidentais de dados de clientes e de trabalhadores, multas e riscos reputacionais inerentes. Só assim será possível criar um ambiente de trabalho próspero e capaz de atrair e reter talentos.

Contudo, e ao contrário do que muitos ainda hoje julgam, a conformidade com o RGPD e com a demais legislação nacional em matéria de proteção de dados não é alcançável através da mera revisão de políticas internas, de contratos, de declarações de consentimento, etc. Igualmente importante é criar mecanismos internos de auditoria, procedimentos que prevejam o fluxo dos dados, os acessos, os pontos de controlo, etc., o que apenas é possível mediante a aplicação das regras legais ao funcionamento dos sistemas de tecnologias de informação (TI) e a criação de procedimentos internos auditáveis.

Assim, surgiu a ideia de criar um guia que associasse e aplicasse a temática da proteção de dados aos recursos humanos – uma associação de conceitos que tem suscitado infindáveis dúvidas aos clientes que assessoramos.

Em conjunto, e de acordo com a nossa experiência profissional, procurámos reunir os principais pontos, as dúvidas e os anseios que os clientes reiteradamente nos colocam, quer os relacionados com a gestão diária dos problemas relativos à contratação e gestão de recursos humanos, quer

aquando da realização de um processo de auditoria e/ou de implementação da conformidade com o RGPD.

Com o intuito de explicar e “descomplicar” matérias que por vezes são densas e polifacetadas, focámo-nos na criação de um guia que fosse de consulta rápida e eficaz para todos os que lidam com processos de recrutamento e de contratação de pessoal, pois agora, mais do que nunca, além de se gerirem pessoas, é preciso gerir dados pessoais.

A análise contida neste guia tem cariz generalista, pelo que a sua leitura não dispensa a consulta de técnicos qualificados em cada uma das matérias contidas no mesmo, os quais poderão enquadrar e analisar as várias soluções possíveis para cada caso concreto.

Esperamos que encontrem neste livro as soluções para resolver os problemas e as dúvidas que, recorrentemente, tanto assolam departamentos de recursos humanos como trabalhadores.