



Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Miguel Filipe Alves Ferreira Lucas

Implementação do RGPD no Setor Empresarial

Implementação do RGPD no Setor Empresarial

Miguel Filipe Alves Ferreira Lucas

ISCAC | 2022

Coimbra, janeiro de 2022



Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade
e Administração de Coimbra

Miguel Filipe Alves Ferreira Lucas

Implementação do RGPD no Setor Empresarial

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Solicitadoria, realizado sob a orientação do Professor Doutor Armando Ferreira Soares Veiga.

Coimbra, janeiro de 2022

TERMO DE RESPONSABILIDADE

Eu, Miguel Filipe Alves Ferreira Lucas, aluno n.º 2019116707, do mestrado em Solicitação, declaro que sou o único autor do trabalho intitulado “Implementação do RGPD no Setor Empresarial”, apresentado no Instituto Superior de Contabilidade e Administração de Coimbra.

Declaro ainda que este trabalho é original e inédito, que os autores e os trabalhos utilizados estão devidamente citados no texto e incluídos na lista final de referências.

Declaro também que quando utilizei frases, ideias, dados ou outras informações de trabalhos de outros autores, indiquei sempre a fonte original. Deste modo, declaro que não há qualquer plágio, não fiz cópia fraudulenta e não apresento como sendo meu o trabalho de outros.

Por fim, declaro que este trabalho, parcialmente ou na totalidade, não foi submetido para outra finalidade.

Coimbra, 31 de janeiro de 2022

DEDICATÓRIA

À minha mãe

AGRADECIMENTOS

À minha mãe e avós pelo amor, incentivo e apoio incondicional. Tudo o que sou hoje a vós vos devo.

À minha namorada, por ser incansável e nunca me deixar desistir.

Uma palavra especial ao meu orientador Senhor Professor Armando Veiga pela disponibilidade, ajuda e ensinamentos.

Um agradecimento também a todos os docentes do ISCAC e da ESGIN, assim como a todos os amigos e colegas que me têm acompanhado nesta jornada.

A todos o meu bem-haja¹!

¹ Expressão tipicamente beirã.

RESUMO

Apesar do Regulamento Geral sobre a Proteção de Dados (RGPD) já se encontrar a produzir efeitos desde o dia 25 de maio de 2018, à data de hoje, são ainda muitas as empresas que têm dificuldades em compreender o conteúdo e aplicação deste. Neste sentido, temos como principal objetivo deste trabalho a análise do conteúdo do RGPD, bem como da Lei n.º 58/2019, de 08 de agosto, que assegura a sua execução no ordenamento jurídico português, com vista à aplicação no contexto laboral.

Deste modo serão explorados, ao longo da dissertação, quais os princípios que revestem a proteção de dados pessoais, os direitos atribuídos aos titulares dos dados pessoais (com a intenção de conceder a estes um maior controlo sobre os seus dados), bem como as especificidades das operações de tratamento realizadas, tanto no âmbito dos processos de recrutamento, como no âmbito da monitorização dos trabalhadores (nomeadamente no que diz respeito à licitude dessas operações). Relativamente controlo dos trabalhadores, realizado dentro e fora do local de trabalho, daremos especial destaque às operações de tratamento de dados pessoais resultantes da utilização de sistemas biométricos, de controlos médicos, de sistemas de geolocalização, de sistemas de videovigilância, e ainda do regime de teletrabalho.

Resumidamente, podemos considerar que o conteúdo desta dissertação tem como objetivo principal a verificação de *compliance* com as normas constantes do RGPD, no setor empresarial.

Palavras-chave: Regulamento Geral de Proteção de Dados (RGPD); Contexto Laboral; Monitorização dos trabalhadores; *Compliance*;

ABSTRACT

Although the General Data Protection Regulation (GDPR) has already taken effect since May 25th, 2018, to date, many companies still struggle with understanding its content and application. In this sense, the main objective of this work is to analyze the content of the GDPR, as well as of the Law number 58/2019, of August 8th, which ensures its implementation in the Portuguese legal system, with the aim of its application in the labor context.

In this way, we will explore, throughout this dissertation, the principles that cover the protection of personal data, the rights attributed to the holders of personal data (with the intention of granting them greater control over their data), as well as the specificities of the processing operations carried out, both in the context of recruitment processes and in the context of employee monitoring (namely with regard to the lawfulness of these operations). Regarding the control of workers, carried out inside and outside the workplace, we will give special emphasis to the operations of processing personal data resulting from the use of biometric systems, medical controls, geolocation systems, video surveillance systems, and also the telecommuting.

Briefly, we can consider that the content of this dissertation has as main objective the verification of compliance with the rules contained in the GDPR, in the business sector.

Keywords: General Data Protection Regulation (GDPR); Labor context; Employee monitoring; *Compliance*;

ÍNDICE GERAL

INTRODUÇÃO	1
1 Evolução Histórica da Proteção de Dados na União Europeia.....	3
2 A Proteção de Dados Pessoais no Ordenamento Jurídico Português	7
2.1 A Constituição da República Portuguesa.....	7
2.2 Código Civil.....	9
2.3 Código de Trabalho	9
3 O Regulamento Geral sobre a Proteção de Dados (RGPD).....	11
3.1 Conceitos	13
3.1.1 Dados Pessoais.....	13
3.1.2 Tratamento	14
3.1.3 Limitação do Tratamento.....	14
3.1.4 Definição de Perfis.....	14
3.1.5 Pseudonomização.....	16
3.1.6 Responsável pelo tratamento	17
3.1.7 Subcontratante	17
3.1.8 Consentimento	18
3.1.9 Violação de dados pessoais.....	18
3.1.10 Regras vinculativas aplicáveis às empresas	19
3.1.11 Autoridade de controlo	19
3.2 Princípios	19
3.2.1 Princípio da licitude, lealdade e transparência.....	20
3.2.2 Princípio da limitação da finalidade	22
3.2.3 Princípio da minimização	23
3.2.4 Princípio da exatidão	24

3.2.5	Princípio da conservação	24
3.2.6	Princípio da integridade e confidencialidade.....	25
3.2.7	Princípio da responsabilidade	26
3.3	Direitos dos titulares	27
3.3.1	Direito de acesso	28
3.3.2	Direito de retificação	29
3.3.3	Direito ao apagamento	30
3.3.4	Direito à limitação do tratamento	32
3.3.5	Direito à portabilidade	33
3.3.6	Direito de oposição	34
3.3.7	Direito a não ser avaliado com base em tratamento automático.....	36
3.4	O Responsável pelo Tratamento e o Subcontratante	36
3.5	Avaliação de Impacto sobre a Proteção de Dados	40
3.6	Autoridade de Controlo	42
4	Tratamento de Dados Pessoais no Contexto Laboral	48
4.1	Enquadramento	48
4.2	Os Fundamentos de Licitude de Tratamento de Dados	51
4.3	Processos de Recrutamento	57
4.3.1	Tratamento de Dados Pessoais	57
4.3.2	Período de Conservação de Currículos	62
4.4	Monitorização dos Trabalhadores Dentro e Fora do Local de Trabalho	65
4.4.1	Sistemas Biométricos.....	66
4.4.2	Controlos Médicos.....	68
4.4.3	Sistemas de Geolocalização.....	71
4.4.4	Sistemas de Videovigilância.....	74
4.4.5	Teletrabalho	77

CONCLUSÃO	81
BIBLIOGRAFIA	83

Lista de abreviaturas, acrónimos e siglas

ADP - Autoridades de Proteção de Dados

AIPD - Avaliação de Impacto sobre a Proteção de Dados

Al. ou al. - Alínea

Art. ou art.- Artigo

ATM - *Automatic Teller Machine*

CC - Código Civil

CdE - Conselho da Europa

CDFUE - Carta dos Direitos Fundamentais da União Europeia

CEDH - Convenção Europeia dos Direitos do Homem

CNIL - Comissão Nacional de Informática e Liberdade Francesa

CNPD - Comissão Nacional de Proteção de Dados

CRP - Constituição da República Portuguesa

CT - Código de Trabalho

CV - *Curriculum Vitae*

GPS - *Global Positioning System* ou Sistema de Posicionamento Global

GSM - *Global System for Mobile Communications* ou Sistema Global para Comunicações Móveis

IP - *Internet Protocol*

MDM - *Mobile Device Management*

N.º ou n.º - Número

RGPD e Regulamento - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016

ss - seguintes

UE - União Europeia

INTRODUÇÃO

A presente dissertação enquadra-se na componente não letiva, correspondente ao 2.º ano do Mestrado em Solicitadoria, ministrada no Instituto Superior de Contabilidade e Administração de Coimbra (ISCAC). O tema escolhido, intitulado “*Implementação do RGPD no Setor Empresarial*”, parte da importância, cada vez mais notória, que os dados pessoais representam para o mundo em que vivemos, mais concretamente, da utilização dos mesmos no contexto laboral.

Nas últimas décadas tem-se assistido a um crescimento tecnológico bastante notório, a era digital que outrora foi um futuro distante torna-se hoje na realidade com que convivemos diariamente. Esta transição trouxe consigo uma panóplia de benefícios que são inegáveis, que acarreta, ao mesmo tempo, uma série de desafios com os quais a sociedade ainda está a aprender a lidar. Talvez um dos maiores diga respeito aos dados pessoais e à sua utilização. A constante e rápida digitalização do mundo veio expor grandes fragilidades no que toca ao tratamento dos dados pessoais e torna-se cada mais importante salvaguardar/promover a proteção dos direitos fundamentais, especialmente no que concerne ao direito à reserva da vida privada. Foi neste sentido que a UE se viu pressionada a proceder à atualização das normas estatuídas na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Assim, a 27 de abril de 2016, surgiu o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (RGPD), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Este Regulamento veio estabelecer um novo paradigma no que diz respeito aos direitos dos titulares dos dados, atribuindo-lhes um maior controlo sobre os mesmos. Para além disto, o mesmo Regulamento contém ainda na sua constituição outras alterações igualmente importantes, que também merecem o seu devido destaque, como é o caso da aplicação de coimas. No entanto, e apesar do RGPD já se encontrar a produzir efeitos desde o dia 25 de maio de 2018, à data de hoje, são ainda muitas as empresas que têm dificuldades em compreender o conteúdo e aplicação deste Regulamento e as respetivas normas.

Através desta análise, pretendemos esclarecer quais os princípios basilares da proteção de dados pessoais, quais os direitos atribuídos aos titulares dos dados e a forma como podem usufruir destes, e ainda quais as especificidades da monitorização dos

Implementação do RGPD no Setor Empresarial

trabalhadores, e respetivo tratamento de dados, de forma a garantir a conformidade com o RGPD.

A dissertação encontra-se estruturada em quatro capítulos distintos, da seguinte forma:

O primeiro capítulo tem como objetivo a realização de um enquadramento da evolução histórica da proteção de dados na UE.

No segundo analisaremos quais os normativos relativos à proteção de dados pessoais atualmente em vigor no ordenamento jurídico português.

De seguida, no terceiro capítulo, será realizada uma abordagem mais aprofundada do RGPD, mais concretamente no que diz respeito aos conceitos que este introduz, aos princípios basilares da proteção de dados, bem como aos direitos dos titulares dos dados. No entanto, ressalva-se ainda a importância da figura do responsável pelo tratamento de dados e das suas competências, bem como as situações das quais resulta a necessidade da realização de avaliações de impacto sobre a proteção de dados.

No quarto e último capítulo, serão abordadas questões mais específicas relativamente ao tratamento de dados pessoais realizado no contexto laboral (como por exemplo quais os fundamentos de licitude dos mesmos). Não obstante, serão analisadas as operações de tratamento realizadas durante o processo de recrutamento, tal como as operações de tratamento resultantes da monitorização dos trabalhadores, dentro e fora do local de trabalho.

1 Evolução Histórica da Proteção de Dados na União Europeia

Com o final do século XX e a evolução das tecnologias de informação (TIC), o tema da proteção de dados foi ganhando, cada vez mais, um lugar de elevada importância debaixo do holofote. O tema da proteção de dados, ainda que atual, manifestou-se pela primeira vez pouco tempo após a Segunda Guerra Mundial. Em 1945, a Europa atravessava uma época marcada pelo conflito que acabara de terminar, bem como pelas consequências que dele advieram, eurgia a necessidade de promover o Estado de direito, a democracia e os direitos humanos.² De forma a colmatar estas necessidades foi, em 1948, adotada pela Organização das Nações Unidas a Declaração Universal dos Direitos do Homem (CUCH), e em 1950, adotada pelo Conselho da Europa (CdE)³, a Convenção Europeia dos Direitos do Homem (CEDH) (que apenas entrou em vigor três anos depois).

É, assim possível, através da epigrafe do artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH), identificar a indispensabilidade da reserva do direito ao respeito pela vida privada e familiar, bem como pelo domicílio e pela correspondência. Mesmo que de uma forma indireta, o direito à proteção de dados faz parte dos direitos consagrados na CEDH, sendo esta, para muitos, a primeira manifestação do direito à proteção de dados pessoais.

Em 1981 (um ano após a adoção das Diretrizes sobre a Proteção da Privacidade e os Fluxos Transfronteiriços de Dados Pessoais por parte da Organização para a Cooperação e Desenvolvimento Económico (OCDE)) o Conselho da Europa (CdE) adotou a Convenção 108 do Conselho da Europa, respeitante ao Tratamento Automatizado de Dados Pessoais. A “(...) *crecente necessidade de adotar regras mais pormenorizadas para salvar-guardar as pessoas através da proteção dos seus dados (pessoais)*”, que levou à adoção da referida Convenção, foi uma consequência direta da evolução das tecnologias de informação que se verificou das décadas de 60 e 70.⁴

² SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 3, Lisboa, FCA - Editora de Informática.

³ Criado em 1949, o Conselho da Europa (mais antiga instituição europeia em funcionamento), era inicialmente composto por 10 países, sendo atualmente composto por todos os Estados Membros da União Europeia (UE). Disponível em <https://www.coe.int/pt/web/about-us/our-member-states>, consultado em 06 de maio de 2020.

⁴ Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), “*Manual da Legislação Europeia sobre a Proteção de Dados*”, Luxemburgo, Serviço de Publicações da União Europeia, p. 17.

Implementação do RGPD no Setor Empresarial

A “*Convenção 108 era (...) o único instrumento internacional juridicamente vinculativo no domínio da proteção de dados*” com o intuito de garantir a proteção dos direitos e liberdades fundamentais das pessoas singulares, no âmbito do tratamento automatizado de dados⁵. Veio dessa forma introduzir alguns princípios, que mantêm a sua relevância até aos dias de hoje, como por exemplo, a licitude da recolha dos dados e do seu tratamento, a compatibilidade dos fins a que se destina o tratamento, com a recolha, bem como a sua legitimidade, o tempo de conservação desses dados e ainda a adequação do mesmo, devendo estes ser pertinentes e exatos.⁶ Para além disso, a Convenção apresenta “*(...) garantias relativas aos dados sensíveis, como raça, opinião política, saúde, convicções religiosas, vida sexual ou registo criminal*”⁷, prevendo, no caso de ausência de garantias jurídicas adequadas, a proibição do seu tratamento.⁸

Com o avançar do tempo, alguns Estados-Membros tomaram a iniciativa de criar normativas sobre esta temática, originando assim alguma discordância entre eles. Estas discrepâncias foram a razão pelo qual foi, no dia 24 de outubro de 1995, aprovada a Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, que tinha como principal objetivo a harmonização das legislações nacionais.⁹

Tal como é possível depreender através da leitura dos Considerandos 1, 4, 7 e 8 da referida Diretiva, a uniformização era necessária, tendo em vista: a coordenação das legislações dos Estados-Membros, garantir a existência de respeito pelo tratamento, equivalente a todos eles, e assegurar que a circulação de dados pessoais, resultante de diversas áreas das atividades económicas e sociais, fosse regulada de forma coerente. A inexistência desta harmonização e consequentes diferenças entre Estados-Membros, poderiam constituir um obstáculo ao exercício de uma série de atividades económicas e

⁵ “A *Convenção 108 aplica-se a todos os tratamentos de dados pessoais realizados tanto pelo setor privado como pelo setor público, incluindo os tratamentos de dados efetuados pelas autoridades policiais e judiciárias*”, cfr. Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), “*Manual da Legislação Europeia sobre a Proteção de Dados*”, Luxemburgo, Serviço de Publicações da União Europeia, p. 16.

⁶ *Idem*, p. 16.

⁷ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 4, Lisboa, FCA - Editora de Informática.

⁸ Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), “*Manual da Legislação Europeia sobre a Proteção de Dados*”, Luxemburgo, Serviço de Publicações da União Europeia, p. 16.

⁹ “*(...) não se limitava a uma harmonização mínima, mas antes conduzia a uma harmonização que era, em princípio, completa*”. ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 15.

Implementação do RGPD no Setor Empresarial

sociais, indispensáveis para atingir objetivos como “(...) *uma união cada vez mais estreita entre os povos europeus (...)*”, “(...) *progresso económico e social (...)*” e a eliminação de “(...) *barreiras que dividem a Europa (...)*”.¹⁰ Para além disso esta Diretiva “*incluiu e desenvolveu ainda mais os princípios gerais da Convenção 108, ao mesmo tempo em que fornece uma abordagem comum para regulamentação e controle pelas autoridades de proteção de dados*”.¹¹

Em 2000, a União Europeia aprovou a Carta dos Direitos Fundamentais da União Europeia (CDFUE), resultante da inexistência de referências à temática dos Direitos Humanos, até à data. Mas foi após a entrada em vigor do Tratado de Lisboa¹², que a CDFUE se tornou juridicamente vinculativa como direito primário da União Europeia, que fixou no seu artigo 7.º e 8.º, o respeito pela vida privada e familiar e a proteção de dados pessoais, respetivamente.¹³ Podemos, neste sentido, citar Nuno Saldanha, quando refere que “(...) *a CDFUE consagra como direito fundamental na UE o direito à proteção dos dados pessoais (...)*”.

Atualmente, vigora o 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 de dados (doravante denominado de RGPD), e que veio, por sua vez, revogar a Diretiva 95/46/CE do Parlamento Europeu e do Conselho. Importa salientar que até à criação deste Regulamento, a Diretiva de Proteção de Dados Pessoais era o “(...) *principal instrumento jurídico da UE sobre proteção de dados (...) no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (...)*”.¹⁴

¹⁰ Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.

¹¹ Traduzido de “*it included and further developed the general principles of Convention 108, while also providing a common approach to regulation and control by the data protection authorities*”, cfr. DE HERT, PAUL & LAMMERAN, Hans (2013), “*Protection of Personal Data in Work-Related Relations*”, p. 14. Disponível em [https://www.europarl.europa.eu/thinktank/pt/document/IPOL-LIBE_ET\(2013\)474440](https://www.europarl.europa.eu/thinktank/pt/document/IPOL-LIBE_ET(2013)474440), acedido a 29 de janeiro de 2022.

¹² O Tratado de Lisboa, que entrou em vigor a 1 de dezembro de 2009, “(...) *fornece uma base mais sólida para o desenvolvimento de um sistema de proteção de dados mais eficaz e mais claro e simultaneamente prevê novos poderes para o Parlamento, que se tornou colegislador*”. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf, acedido 26 de janeiro de 2022.

¹³ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 5, Lisboa, FCA - Editora de Informática.

¹⁴ Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), “*Manual da Legislação Europeia sobre a Proteção de Dados*”, Luxemburgo, Serviço de Publicações da União Europeia, p. 18.

Implementação do RGPD no Setor Empresarial

A necessidade de atualizar as normas relativas à proteção de dados pessoais proveio dos novos desafios criados pela rápida evolução tecnológica e pela globalização.¹⁵ Por sua vez, e como é possível reter da leitura no Considerando 7 deste regulamento, esta evolução exigiu um quadro de proteção sólido e mais coerente, apoiado por uma rigorosa aplicação das regras.

¹⁵ Considerando 6 do RGPD.

2 A Proteção de Dados Pessoais no Ordenamento Jurídico Português

As alterações e atualizações, que se verificaram no contexto europeu, tiveram repercussões nos Estados-Membros e na composição dos seus textos jurídicos. Neste sentido, e uma vez que Portugal não é exceção, possui diversas referências à proteção de dados em distintos textos jurídicos. Destes, são de especial interesse para a compreensão da temática da proteção de dados no contexto laboral, as inseridas na Constituição da República Portuguesa (CRP), no Código Civil (CC), no Código de Trabalho (CT) e posteriormente na Lei n.º 58/2019, de 8 de agosto¹⁶.

2.1 A Constituição da República Portuguesa

Citando Carlos Manuel Carvalho dos Santos, “*o direito da privacidade compreende a proteção de dados pessoais*”¹⁷, estando ambos defendidos na Constituição da República Portuguesa, mais especificamente nos art. 26.º e 35.º, respetivamente.

Assim, nos termos do artigo 26.º da Constituição da República Portuguesa, entre outros¹⁸, a todos é reconhecido o direito à reserva da intimidade da vida privada e familiar (n.º 1 referido artigo).¹⁹ Neste contexto devemos sempre ter em conta que o “(...) *direito fundamental à reserva da intimidade da vida privada e familiar deverá delimitar-se (...) como base num conceito de «vida privada» que tenha em conta a referência civilizacional sob três aspetos: (1) o respeito dos comportamentos; (2) o respeito do anonimato; (3) o respeito da vida em relação*”.²⁰ Estes pontos tornam-se essenciais na análise de situações

¹⁶ Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento 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.

¹⁷ SANTOS, Carlos Manuel Carvalho dos (2015), “*Proteção de Dados dos Trabalhadores*”, Lisboa, Universidade Autónoma de Lisboa, p. 13. Disponível em <https://repositorio.ual.pt/bitstream/11144/1856/1/Prote%20de%20Dados%20dos%20Trabalhadores.pdf>, acessado a 15 de abril de 2021.

¹⁸ O artigo 26.º, n.º 1 da CRP, inclui na sua estrutura “(...) *nove direitos distintos (...)*”. CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume 1*”, 4.ª Edição Revista, p. 461, Coimbra, Almedina.

¹⁹ Este direito de personalidade está diretamente ligado ao princípio da dignidade humana, na medida em que a pessoa beneficé de um espaço de privacidade, quer no âmbito da vida doméstica, familiar, sexual ou afetiva, cfr. PAIS DE VASCONCELOS, Pedro (2019), “*Teoria Geral do Direito Civil*”, 9.ª Edição, Coimbra, Edições Almedina, p. 63. ISBN 9789724081847

²⁰ CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume 1*”, 4.ª Edição Revista, p. 468, Coimbra, Almedina.

das quais pode resultar a violação deste direito, ganhando uma importância ainda maior, como será possível observar ao longo desta Dissertação, no âmbito das relações jurídico-laborais. Deste modo, no que diz respeito à reserva da intimidade da vida privada e familiar, podemos afirmar que os pontos acima transcritos consubstanciam na aplicação do princípio da proporcionalidade (nos termos do artigo 18.º, n.º 2 da CRP).²¹

No entanto, o artigo 26.º da CRP acrescenta ainda que fica a lei responsável pelo estabelecimento de “(...) *garantias efetivas contra a obtenção e utilização abusiva, ou contrárias à dignidade humana, de informações relativas a pessoas e famílias*” (n.º 2 do referido artigo). O Código Civil, no seu artigo 80.º, introduz uma dessas garantias, no que diz respeito à reserva da intimidade da vida privada e familiar (n.º 1 do referido artigo).²²

Relativamente à utilização da informática, o artigo 35.º n.º 1 da CRP prevê, a todos, “(...) *o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam (...)*”²³. No que diz respeito ao tratamento de dados pessoais, podemos considerar esta atribuição do artigo 35.º da CRP, como “(...) *uma espécie de direito básico (...)*” que remete para os direitos dos titulares dos dados nos termos do RGPD²⁴. Referimo-nos particularmente ao direito de acesso do titular dos dados (artigo 15.º do RGPD), ao direito ao conhecimento da identidade dos responsáveis (artigo 13.º, n.º 1, alínea a) e artigo 14.º, n.º 1, alínea a) do RGPD), ao direito ao esclarecimento sobre a finalidade a que se destinam os dados (artigo 13.º, n.º 1, alínea c), artigo 14.º, n.º 1, alínea c) e artigo 15.º, n.º 1, alínea a) do RGPD), ao direito à retificação dos dados (artigo 16.º do RGPD), ao direito ao apagamento (artigo 17.º do RGPD), ao direito à limitação dos dados (artigo 18.º do RGPD), entre outros.²⁵

²¹ Cfr. HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “*Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*”, “*Anuário de Proteção de Dados*”, p. 15. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 29 de janeiro de 2022.

²² CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume I*”, 4.ª Edição Revista, p. 471, Coimbra, Almedina.

²³ Também conhecido por direito à autodeterminação informativa.

²⁴ Ver páginas 27 a 35 desta Dissertação.

²⁵ CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume I*”, 4.ª Edição Revista, pp. 551-552, Coimbra, Almedina.

2.2 Código Civil

O Código Civil, no seu artigo 70.º, menciona que “*a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral*”. Podemos então depreender que, o direito à imagem (artigo 79.º do CC), bem como o direito à reserva sobre a intimidade da vida privada (artigo 80.º do CC), se encontram compreendidos no conteúdo do artigo 70.º do CC.

Neste sentido, no que diz respeito ao direito à reserva da vida privada, o n.º 1 do artigo 80.º do CC enuncia que a todos cabe a obrigação de guardar reserva quando à intimidade da vida privada de outrem, sob pena de aplicação de sanções penais (artigo 190.º, n.º 2 do Código Penal).²⁶

2.3 Código de Trabalho

Por sua vez, o Código de Trabalho (CT) introduz no n.º 1 do seu artigo 16.º a obrigação de respeito mútuo entre os trabalhadores e a entidade empregadora, no que concerne aos direitos de personalidade, bem como à reserva da intimidade da vida privada, de ambos. As normas constantes do CT com vista à defesa de direitos de personalidade dos trabalhadores encontram-se consagrados nos artigos 16.º a 22.º do mesmo, e abrangem desde a proteção de dados, na sua conceção, à proteção de dados em situações específicas, como por exemplo na proteção de dados biométricos (artigo 18.º do CT) ou na utilização de meios de vigilância a distância (artigos 20.º e 21.º do CT).

No que diz respeito à reserva da intimidade da vida privada, o n.º 2 do artigo 16.º do CT acrescenta que estes “*(...) abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas*”.

Tal como referido anteriormente, e de forma a garantir a proteção dos dados pessoais dos trabalhadores, o CT acrescenta ainda no artigo 17.º que a entidade

²⁶ CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume I*”, 4.ª Edição Revista, p. 471, Coimbra, Almedina.

Implementação do RGPD no Setor Empresarial

empregadora se encontra impedida de solicitar aos seus trabalhadores informações relacionadas com a sua vida privada (excetuando as situações em que o seu tratamento é considerado relevante e necessário para a avaliação da sua aptidão na execução do contrato de trabalho), bem como informações relacionadas com a sua saúde (salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem, e apenas quando prestadas a médico especialista em medicina no trabalho²⁷) (alíneas a) e b) do n.º 1 do referido artigo). Esta limitação resulta do risco que representa, para os respetivos titulares, o tratamento destes dados, agrupando-se estes numa categoria de dados distinta dos restantes.

²⁷ Art. 17.º, n.º 2 do CT.

3 O Regulamento Geral sobre a Proteção de Dados (RGPD)

Como referido anteriormente, os avanços tecnológicos, a aprovação da Carta dos Direitos Fundamentais da União Europeia (CDFUE) e do Tratado de Lisboa, entre outros fatores, levaram à inevitável revisão da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.²⁸ Através da leitura da “*Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da proteção de dados pessoais na União Europeia*”²⁹ é possível compreender a necessidade de uma reforma e harmonização das normas de proteção de dados existentes até então.³⁰ No seu conteúdo foram ainda assinaladas várias questões problemáticas que mereceram a devida análise ao longo da referida Comunicação, das quais resulta a necessidade de: equacionar impacto das novas tecnologias; reforçar a vertente de proteção de dados do mercado interno; equacionar a globalização e melhorar as transferências de dados internacionais; conseguir um quadro institucional mais firme para a aplicação efetiva das normas de proteção de dados; e aumentar a coerência do quadro normativo que rege a proteção de dados.³¹ A referida reforma e consequente modernização das normas implicou um aprofundamento dos princípios constantes da Diretiva, de forma a garantir uma proteção adequada aos novos desafios apresentados pela globalização e consequente aumento do fluxo transfronteiriço de dados³². Neste sentido foi, a 27 de abril de 2016, publicado o Regulamento (EU)

²⁸ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 81.

²⁹ Ver “*Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da proteção de dados pessoais na União Europeia*”, disponível em <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52010DC0609>., acedido a 03 de março de 2021.

³⁰ “*As pretensões da Comissão foram aplaudidas e apoiadas pelo Parlamento que instou a Comissão a assegurar que “a atual revisão da legislação de proteção de dados da EU preveja: - uma harmonização plena, ao mais alto nível, que ofereça segurança jurídica e um nível de proteção das pessoas elevado e uniforme em todas as circunstâncias”*”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 82.

³¹ Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da proteção de dados pessoais na União Europeia (2011/2025(INI)) pp. 3-4. Disponível em https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323_PT.html, acedido a 03 de março de 2021.

³² Que teve como consequência “(...) *uma cada vez maior integração económica, fruto, sem dúvida, da criação do mercado único, mas também em resultado de um intercâmbio de dados que se verifica cada vez mais entre sectores público e privado, de maior recolha e partilha de dados, tidos já como um valor económico muito real e mensurável, e a utilização, por todas as organizações, sejam públicas ou privadas, de dados pessoais em larga escala*”, cfr. SALDANHA, Nuno (2018), “*Novo Regulamento Geral de*

Implementação do RGPD no Setor Empresarial

2016/679 do Parlamento Europeu e do Conselho³³, que pretende, para além de garantir a livre circulação de dados entre os Estados-Membros, criar uma aplicação uniforme em toda a UE³⁴. No entanto, de forma a atingir essa uniformização é necessária uma aplicação rigorosa das normas constantes neste Regulamento (Considerando 7 do RGPD).

Ao contrário da Diretiva 95/46/CE, a figura do Regulamento não carece de uma transposição por parte dos Estados-Membros, uma vez que “(...) *é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da EU*”³⁵. Ou seja, o RGPD é responsável pela criação de um quadro legal mais coeso e homogêneo, apesar de, na sua versão final, conter “(...) *recorrentes cláusulas de abertura - medidas legislativas facultativas de índole substantiva - em benefício dos Estados-Membros e da própria União*”^{36,37}.

Para além de introduzir um novo paradigma no que diz respeito aos direitos dos titulares dos dados, a maior novidade do RGPD é a introdução de coimas a ser aplicadas aquando do incumprimento das obrigações impostas. O valor destas coimas, que podem chegar aos 20.000.000,00€ ou aos 4% do volume de negócios anual (correspondente ao exercício financeiro anterior) (n.º 5 do artigo 83.º do RGPD), vêm de certa forma criar alguma preocupação e necessidade de cumprir/aplicar as normas necessárias em conformidade com o RGPD.

No que diz respeito ao âmbito de aplicação deste Regulamento, devemos ter em conta que o mesmo se aplica ao tratamento de dados pessoais efetuados “(...) *por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados*” (artigo 2.º, n.º 1 do RGPD), “(...) *no contexto das atividades de um estabelecimento de um*

Proteção de Dados: O que é? A quem se aplica? Como implementar?”, s.e., p. 15, Lisboa, FCA - Editora de Informática.

³³ Mais conhecido por Regulamento Geral sobre a Proteção de Dados, veio revogar a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>, acessado a 19 de Fevereiro de 2021.

³⁴ Ver Considerando 10 do RGPD.

³⁵ Ver Comissão Europeia (s.d.), “*Regulamentos, diretivas e outros atos legislativos*”. Disponível em https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt, acessado a 26 de maio de 2021.

³⁶ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 83.

³⁷ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 16, Lisboa, FCA - Editora de Informática.

responsável pelo tratamento (...) situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União” (artigo 3.º, n.º 1 do RGPD).

3.1 Conceitos

O atual RGPD, tal como já a Diretiva 95/46/CE fazia menção no seu artigo 2.º (apesar que de uma forma menos abrangente e mais superficial), elenca, no seu artigo 4.º, as definições necessárias para a compreensão do mesmo. Este artigo tem como objetivo a fixação das definições das expressões nele elencadas, delimitando possíveis variações quanto ao significado das mesmas. Neste sentido, para uma melhor compreensão da seguinte dissertação é necessário abordar algumas das definições elencadas ao longo do artigo 4.º do RGPD.

3.1.1 Dados Pessoais

Por dados pessoais devemos compreender que são toda a “*informação relativa a uma pessoa singular identificada ou identificável (...)*” (n.º 1 do artigo 4.º do RGPD). Para além disso, o n.º 1 do referido artigo acrescenta ainda que “*(...) é identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (...)*”. Um exemplo de dado pelo qual pode a pessoa ser diretamente identificada é o seu nome³⁸, já no que diz respeito aos dados pelos quais será possível identificar indiretamente uma pessoa, podemos dar como exemplo o número de telefone ou até a matrícula de um veículo.³⁹

Em síntese, pode ser considerado dados pessoais, um nome (seja nome próprio ou apelido), um número de identificação (n.º de Cartão de Cidadão ou Bilhete de Identidade, número de identificação fiscal (NIF), número de utente, entre outros...), endereços de residência, endereço de correio eletrónico, identificadores por via eletrónica (dados de localização de um *smartphone*, endereço de IP, *cookies*), entre muitos outros.⁴⁰

³⁸ Ressalve-se que se se tratar de “*(...) um apelido muito comum não será suficiente para identificar alguém (...)*”, sendo por isso necessário ter em conta o contexto da situação. Cfr. Grupo de Trabalho do Artigo 29.º - “*Parecer 4/2007 sobre o conceito de dados pessoais*”, adotado em 20 de junho, p. 13.

³⁹ Grupo de Trabalho do Artigo 29.º - “*Parecer 4/2007 sobre o conceito de dados pessoais*”, adotado em 20 de junho, p. 13.

⁴⁰ Comissão Europeia (s.d.), “*O que são dados pessoais?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, acessado a 07 de janeiro de 2022.

No entanto, a definição de dados pessoais acima transcrita, elenca ainda categorias especiais de dados⁴¹, sendo o seu tratamento, nos termos do n.º 1 do artigo 9.º do RGPD, proibido. Por categorias especiais de dados podemos compreender que são todos aqueles “(...) *que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como (...) dados genéticos, dados biométricos (...), dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa*” (n.º 1 do artigo 9.º do RGPD).⁴² Contudo, esta proibição não se aplica às situações estatuídas nas alíneas do n.º 2 do referido artigo.

3.1.2 Tratamento

Por tratamento deve compreender-se que é “(...) *uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*” (n.º 2 do artigo 4.º do RGPD). Um exemplo de operação de tratamento de dados, realizada no contexto laboral, que por sua vez será analisada mais à frente nesta Dissertação, são os sistemas de videovigilância.

3.1.3 Limitação do Tratamento

Limitação do tratamento consiste na “(...) *inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro*” (n.º 3 do art. 4.º do RGPD). Esta é uma forma de garantir uma maior segurança no que toca ao tratamento de dados pessoais.

3.1.4 Definição de Perfis

É “(...) *qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu*

⁴¹ Outrora denominados de *dados sensíveis* (artigo 7.º da Lei n.º 67/98, de 26 de Outubro).

⁴² Comissão Europeia (s.d.), “A proteção de dados ao abrigo do RGPD”, “O que se entende por dados pessoais?”. Disponível em https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm, acessado a 07 de janeiro de 2022.

desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações” (n.º 4 do artigo 4.º do RGPD). Por outras palavras, definição de perfis consiste na avaliação de características dos sujeitos singulares e/ou classificação em categorias, por parte de uma empresa ou organização.⁴³

A definição de perfis e as decisões automatizadas são, cada vez mais, um recurso fundamental, utilizado pelas empresas, principalmente no decorrer dos processos de recrutamento e seleção de novos candidatos. Estes recursos têm como finalidade nomear, de entre todos os sujeitos que se candidataram, o mais apto para desempenhar as funções correspondentes àquele cargo, de forma a evitar perdas de tempo, bem como um aumento de custos desnecessário.⁴⁴ Em suma, como refere a Comissão Europeia, o tratamento automatizado de dados e consequentes decisões podem ser mais eficientes, mas menos transparentes.⁴⁵

O titular dos dados goza, entre outros, do direito de oposição, instituído no artigo 21.º do RGPD, que atribui a este “(...) *o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito (...) incluindo a definição de perfis (...)*”. No entanto, o artigo 22.º do RGPD acrescenta ainda que este “(...) *tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis (...)*”⁴⁶. Não obstante, e de forma a que lhe seja possível o exercício dos seus direitos, o titular dos dados deve ser informado, pelo responsável pelo tratamento, da existência de decisões automatizadas, incluindo a definição de perfis, quer

⁴³ Comissão Europeia (s.d.), “*Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt, acessado a 30 de maio de 2021.

⁴⁴ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 27. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021.

⁴⁵ Comissão Europeia (s.d.), “*Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt, acessado a 30 de maio de 2021.

⁴⁶ No entanto, o estatuído no n.º 1 do art. 22.º do RGPD não se aplica se a decisão: for necessária para a celebração de um contrato ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento; for autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito; ou se for baseada no consentimento inequívoco do titular dos dados (alíneas a), b) e c) do n.º 2 do art. 22.º, respetivamente, em conjunto com o elencado no Considerando 71, ambos do RGPD).

3.1.6 Responsável pelo tratamento

Por responsável pelo tratamento ou *controller*⁵³ podemos entender que é “(...) a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais (...)” (n.º 7 do artigo 4.º do RGPD). Como o próprio nome sugere, trata-se da pessoa responsável pela determinação dos fins a que se destinam os dados pessoais⁵⁴, bem como os meios pelos quais estes serão tratados. No caso de se tratar de uma pessoa coletiva, este não será o funcionário ou representante, mas sim a própria pessoa coletiva.⁵⁵ Pode, nas situações em que tal se verifique, o empregador ser considerado responsável pelo tratamento “(...) em relação aos dados dos seus funcionários (...)”⁵⁶, seja em situações decorrentes do cumprimento do contrato de trabalho (diligências contratuais) ou nos processos de recrutamento.

O responsável pelo tratamento está ainda incumbido, quando verifique necessidade para tal, de contratar um subcontratante, para que este desempenha as suas funções.⁵⁷

3.1.7 Subcontratante

Subcontratante, ou *processor*⁵⁸, é “(...) uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes” (n.º 8 do artigo 4.º do RGPD), por outras palavras, é considerado um mandatário do responsável pelo tratamento, ficando, nestes termos, “(...) obrigado a atuar sempre no melhor interesse do beneficiário da relação (...)”⁵⁹.

⁵³ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 73, Lisboa, FCA - Editora de Informática.

⁵⁴ No sentido em que as operações de tratamento devem ser consideradas inerentes às funções desempenhadas pela entidade onde este desempenha as suas funções cfr. Grupo de Trabalho do Artigo 29.º - “*Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*”, adotado em 16 de fevereiro de 2010, p. 14

⁵⁵ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 307

⁵⁶ Grupo de Trabalho do Artigo 29.º - “*Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*”, adotado em 16 de fevereiro de 2010, p. 14

⁵⁷ Esta figura, bem como a do subcontratante, devido à sua importância para a temática do tratamento de dados pessoais, serão abordadas de uma forma mais extensa e aprofundada no nas páginas 36-39 desta Dissertação.

⁵⁸ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 79, Lisboa, FCA - Editora de Informática.

⁵⁹ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 309.

3.1.8 Consentimento

Por consentimento ou consentimento do titular dos dados, expressão pelo qual também é diversas vezes identificado, devemos depreender que é “(...) *uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*” (n.º 11 do artigo 4.º do RGPD).

A definição anteriormente transcrita sofreu, a 04 de março de 2021, uma retificação na versão em língua portuguesa, passando a ler-se “(...) *informada e inequívoca (...)*” ao invés de “(...) *informada e explícita (...)*”.⁶⁰

3.1.9 Violação de dados pessoais

Violação de dados pessoais, ou *data breach*, consiste numa “(...) *violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento*” (n.º 12 do artigo 4.º do RGPD). Por sua vez, por violação de segurança devemos conceber que é um “*evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como um acesso não autorizado ao sistema de informação*”.⁶¹

A violação de dados pode causar ao titular dos mesmos, danos físicos, materiais ou imateriais, como por exemplo, a limitação de direitos, roubo ou usurpação de identidade, perdas financeiras, entre outros.⁶²

No caso de se verificar uma violação de dados pessoais cabe ao responsável pelo tratamento de dados notificar, sem demora injustificada, a autoridade de controlo, no

⁶⁰ Retificação do 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). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2021.074.01.0035.01.POR&toc=OJ:L:2021:074:TOC, acedido a 15 de junho de 2021.

⁶¹ OPENLIMITS (2017), “*RGPD - GLOSSÁRIO: TODOS OS TERMOS QUE PRECISA DE CONHECER*”. Disponível em <https://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protecao-dados/?all=1>, acedido a 12 de maio de 2022.

⁶² Considerando 85 do RGPD.

prazo de 72 horas a contar do conhecimento da mesma, bem como o titular dos dados da violação de dados pessoais.⁶³

3.1.10 Regras vinculativas aplicáveis às empresas

Nos termos do n.º 20 do artigo 4.º do RGPD, as regras vinculativas aplicáveis às empresas consistem em “(...) *regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta*”. Estas regras, aprovadas pela autoridade de controlo de forma a contribuírem para uma aplicação coerente do RGPD em toda a União Europeia (artigo 63.º do RGPD), devem “*ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento*”, “*conferir expressamente aos titulares dos dados os direitos oponíveis relativamente ao tratamento dos seus dados pessoais (...)*” e cumprir os requisitos elencados nas alíneas do n.º 2 do artigo 47.º do RGPD (alíneas a), b) e c) do n.º 1 do artigo 47.º do RGPD, respetivamente).

3.1.11 Autoridade de controlo

Autoridade de controlo, também denominadas por ADP, consiste numa “(...) *autoridade pública independente criada por um Estado-Membro (...)*” (n.º 21 do artigo 4.º do RGPD). Nestes termos, cabe a cada Estado-Membro estabelecer uma ou mais autoridades de controlo (n.º 1 do artigo 51.º do RGPD), sendo que em Portugal, a autoridade de controlo responsável pela aplicação coerente do RGPD é a Comissão Nacional de Proteção de Dados (CNPD).⁶⁴

3.2 Princípios

O tratamento de dados pessoais realizado nos termos do Regulamento Geral da Proteção de Dados obedece a uma série de princípios que, por sua vez, se encontram

⁶³ Considerandos 85 a 87 do RGPD.

⁶⁴ Artigos 3.º e 4.º, n.º 2 da Lei n.º 58/2019, de 8 de agosto.

fundamentais do titular dos mesmos (alíneas b) a f) do n.º 1 do artigo 6.º do RGPD, respetivamente). Através da apreciação das situações acima identificadas é possível constatar que a licitude do tratamento nem sempre depende do consentimento do titular dos dados (principalmente no que concerne ao tratamento de dados efetuado no contexto laboral).

No que concerne ao princípio da lealdade⁶⁸, devemos ter em conta que o mesmo “(...) *está relacionado com o desenvolvimento do tratamento de dados pessoais de uma forma equilibrada tendo em conta os interesses dos responsáveis pelo tratamento e dos subcontratantes, por um lado, e dos titulares dos dados, por outro*”.⁶⁹ Tendo como exemplo as operações de tratamento realizadas com base no consentimento do titular, cabe ao responsável pelo tratamento o ónus de demonstrar esse consentimento (artigo 7.º, n.º 1 do RGPD). No entanto, o consentimento só é presumivelmente livre (nos termos do n.º 11 do artigo 4.º do RGPD), se o mesmo não for inerente à execução de um contrato (artigo 7.º, n.º 4 do RGPD) e se o titular dispuser de toda a informação sobre o tratamento. Não obstante, o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento (artigo 7.º, n.º 3 do RGPD).⁷⁰

Por último, no que diz respeito ao princípio da transparência⁷¹, este implica que todo o processo de tratamento de dados pessoais seja realizado com clareza e sinceridade.⁷² De uma forma mais concisa, “(...) *todas as informações ou comunicações acerca dos direitos do titular dos dados, relacionadas com o tratamento de dados pessoais, devem ser de fácil acesso e compreensão*”⁷³ “(...) *e formuladas numa linguagem clara e simples*”⁷⁴. O Parecer 3/2013 sobre a limitação da finalidade”, adotado em 2 de

⁶⁸ Considerado um “(...) *plus em relação ao princípio da licitude* (...)”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 153

⁶⁹ Diário da República Eletrónico (s.d.), “*Princípio da lealdade (tratamento de dados pessoais)*”. Disponível em <https://dre.pt/dre/lexionario/termo/principio-lealdade-tratamento-dados-pessoais>, acessado a 27 de janeiro de 2022.

⁷⁰ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., pp. 45-46, Lisboa, FCA - Editora de Informática.

⁷¹ Novidade introduzida pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ver Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à transparência na aceção do Regulamento 2016/679*”, adotadas em 29 de novembro de 2017, pp. 4-6.

⁷² CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 154.

⁷³ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 46, Lisboa, FCA - Editora de Informática.

⁷⁴ Considerando 39 do RGPD.

abril de 2013⁷⁵, faz ainda, na sua sétima página, alusão, com a devida importância, ao artigo 12.º do RGPD, no sentido em que, é neste que se encontram definidas as regras aplicáveis: às informações a facultar (por parte do responsável) quando os dados pessoais sejam recolhidos junto do titular (artigo 13.º do RGPD); às informações a facultar quando os dados pessoais não sejam recolhidos juntos do titular (artigo 14.º do RGPD); às comunicações acerca dos direitos do titular dos dados (artigo 15.º a 22.º do RGPD); e às comunicações de violações de dados pessoais (artigo 34.º do RGPD).

3.2.2 Princípio da limitação da finalidade

Este princípio encontra-se elencado na alínea b) do n.º 1 do artigo 5.º do RGPD, onde se encontra elencado, que os dados pessoais são *“recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades (...)”*. A importância da limitação destes fins, ou por outras palavras, da fixação de fins específicos⁷⁶ para o tratamento de dados pessoais, resulta da necessidade de consentimento por parte do titular dos dados (artigo 7.º do RGPD). Isto é, o titular deve ser informado do fim ou fins a que se destina a recolha dos seus dados. Caso este não compreenda a razão da recolha, nem a finalidade do tratamento desses dados, é-lhe impossível dar um consentimento válido⁷⁷. Para além disso, a utilização dos dados recolhidos deve ser compatível com os fins determinados e aceites pelo titular, aquando do seu consentimento, no sentido em que *“o tratamento de dados pessoais para finalidades indeterminadas e/ou ilimitadas é ilícito”*^{78, 79}.

Na parte final da alínea b) do n.º 1 do artigo 5.º do RGPD encontram-se identificadas exceções relativamente ao tratamento posterior, referindo assim que, quando o tratamento seja realizado *“(...) para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é*

⁷⁵ Grupo de Trabalho do Artigo 29.º - *“Parecer 3/2013 sobre a limitação da finalidade”*, adotado em 2 de abril de 2013.

⁷⁶ Art. 8.º, n.º 2 da CDFUE.

⁷⁷ Sendo este um dos preceitos essenciais para a verificação de um consentimento válido, o que por sua vez pode indicar a presença de um tratamento leal. Ver páginas 20 a 21 desta Dissertação.)

⁷⁸ Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), *“Manual da Legislação Europeia sobre a Proteção de Dados”*, Luxemburgo, Serviço de Publicações da União Europeia, p. 73.

⁷⁹ Grupo de Trabalho do Artigo 29.º - *“Parecer 3/2013 sobre a limitação da finalidade”*, adotado em 2 de abril de 2013, pp. 15-17

considerado incompatível com as finalidades iniciais (...)”, desde que em conformidade com o artigo 89.º do RGPD.

As finalidades do tratamento de dados devem ainda, entre outras informações, constar no registo de atividades de tratamento, realizado pelo responsável pelo tratamento ou pelo subcontratante, por escrito e em formato digital/eletrónico, uma vez que o mesmo pode ser requisitado pela CNPD a qualquer altura (artigo 30.º, n.º 1, alínea b), n.º 3 e n.º 4 do RGPD).

3.2.3 Princípio da minimização

O princípio da minimização dos dados, também denominado princípio da qualidade dos dados ou da pertinência dos dados⁸⁰, compreende que os mesmos são *“adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados”* (artigo 5.º, n.º 1, alínea c) do RGPD).⁸¹

Deve ter-se em conta, que apesar deste princípio não ser novo, recebeu com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, uma nova definição mais restrita, não deixando espaço para manobra, tendo sido substituída a expressão *“não excessivos”*⁸² por *“limitados ao que é necessário”*.⁸³

O princípio da minimização dos dados tem como objetivo o tratamento dos mesmos, que se considerem adequados à finalidade para a qual foram recolhidos, e pertinentes no sentido em que *“(…) circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades”*. Não

⁸⁰ SALDANHA, Nuno (2018), *“Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?”*, s.e., p. 47, Lisboa, FCA - Editora de Informática.

⁸¹ O princípio da minimização de dados está *“(…) intrinsecamente associado ao princípio da limitação de finalidades (...)”*, uma vez que os dados são limitados ao que é necessário relativamente às finalidades para as quais são recolhidos e tratados. Cfr. CORDEIRO, A. Barreto Menezes (2020), *“Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019”*, Reimpressão, Coimbra, Almedina, p. 158.

⁸² Onde se podia ler *“adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente”* (alínea c) do n.º 1 do artigo 6.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995).

⁸³ CORDEIRO, A. Barreto Menezes (2020), *“Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019”*, Reimpressão, Coimbra, Almedina, p. 158.

obstante, devem ainda ser considerados necessários, uma vez que pode verificar-se a utilização de meios⁸⁴ que garantam uma maior proteção desses dados.⁸⁵

A forma como são, através do texto da alínea c) do n.º 1 do artigo 5.º do RGPD, enquadrados os dados pessoais, resulta numa menor retenção da informação⁸⁶ e consequente diminuição do risco de perda da mesma (nos casos de violação de dados ou *data breach*). Criando um cenário mais seguro no que toca ao tratamento de dados pessoais.⁸⁷

3.2.4 Princípio da exatidão

O princípio da exatidão, também conhecido por princípio da precisão, determina que os dados pessoais têm de ser “*exatos e atualizados sempre que necessário (...)*” devendo ainda ser garantido, por parte do responsável pelo tratamento, que não serão conservados dados considerados inexatos para as finalidades a que se destinam. Nos casos em que se verifique a conservação destes dados, os mesmos devem ser eliminados⁸⁸ ou retificados pelo titular dos mesmos⁸⁹ (alínea d) do n.º 1 do artigo 5.º do RGPD).

3.2.5 Princípio da conservação

O princípio da conservação, ou princípio da limitação da conservação, estabelece que os dados pessoais devem ser “*conservados de uma forma que permita a identificação*

⁸⁴ A anonimização e a pseudonimização são exemplos desses meios. A anonimização “(...) *é uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa (...)*”, já a pseudonimização é um processo utilizado no “*tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente (...)*”. O objetivo destes meios é a dissociação dos dados, do respetivo titular (ver página 16 desta Dissertação). Universidade de Coimbra (s.d.), “*Informação Administrativa e Proteção de Dados*”; “*Anonimização e Pseudonimização*”. Disponível em https://www.uc.pt/pt/protecao-de-dados/protecao_dados_pessoais/anonimizacao, acessado a 7 de setembro de 2021 & OPENLIMITS (2017), “*RGPD - GLOSSÁRIO: TODOS OS TERMOS QUE PRECISA DE CONHECER*”. Disponível em <https://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protecao-dados/?all=1>, acessado a 12 de maio de 2022.

⁸⁵ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 159.

⁸⁶ A retenção de informação é menor no sentido em que, de entre todas as categorias de dados existentes (anteriormente explanadas nas páginas 13 a 14 desta Dissertação), apenas serão escolhidos e utilizados os dados referentes às categorias mais apropriadas para a finalidade a que se destinam. Ver SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 47, Lisboa, FCA - Editora de Informática.

⁸⁷ *Idem*, p. 47.

⁸⁸ Direito ao apagamento dos dados, também conhecido por direito ao esquecimento, previsto no artigo 17.º do RGPD.

⁸⁹ Direito de retificação dos dados pessoais, previsto no artigo 16.º do RGPD. Ver páginas 29 a 30 desta Dissertação.

dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (...)” (primeira parte da alínea e) do n.º 1 do artigo 5.º do RGPD). Neste sentido, é possível compreender que o objetivo do RGPD/Regulamento é cingir, ao mínimo, o prazo de conservação de dados. Esta limitação não impede que, em situações como o tratamento exclusivo para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (artigo 89.º do RGPD), a conservação de dados pessoais não se verifique por um período mais longo (segunda parte da alínea e) do n.º 1 do artigo 5.º do RGPD).

De forma a garantir que a conservação de dados fique limitada ao período estritamente necessário, e de acordo com o Considerando 39 do RGPD, cabe ao responsável pelo tratamento de dados a fixação dos prazos para o apagamento ou para a revisão periódica.⁹⁰

3.2.6 Princípio da integridade e confidencialidade

O princípio da integridade e confidencialidade, consagrado na alínea f) do n.º 1 do artigo 5.º do RGPD, assegura que os dados pessoais são *“tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas e organizativas adequadas”*. Nesta perspetiva a palavra de ordem é segurança, cabendo ao responsável pelo tratamento a obrigação de garantir que se encontram adotadas todas as medidas e meios necessários para evitar o acesso indevido e a utilização dos dados pessoais por pessoas sem autorização para tal.⁹¹ Tal como se encontra elencado artigo 32.º do RGPD, sob a epígrafe *“segurança do tratamento”*, existem vários métodos à disposição do responsável pelo tratamento (e/ou do subcontratante), sendo esses, a pseudonimização e a cifragem dos dados pessoais; a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; e um

⁹⁰ SALDANHA, Nuno (2018), *“Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?”*, s.e., p. 48, Lisboa, FCA - Editora de Informática.

⁹¹ Diário da República Eletrónico (s.d.), *“Princípio da integridade e confidencialidade”*. Disponível em <https://dre.pt/dre/LinkLexionarioAntigo?termoId=143859891>, acessado a 29 de abril de 2021

processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento (n.º 1 do artigo 32.º do RGPD).

No caso de se verificar uma violação dos dados pessoais, o responsável pelo tratamento tem de notificar a autoridade de controlo competente (neste caso a CNPD) e, no caso da mesma ser suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, deve também comunicar a violação ao titular dos dados (artigos 33.º n.º 1 e 34.º n.º 1, ambos do RGPD). Deve ainda ser feita a ressalva de que ambas as comunicações devem ser efetuadas sem demora injustificada.⁹²

3.2.7 Princípio da responsabilidade

O princípio da responsabilidade, também conhecido por *accountability*, encontra-se elencado no n.º 2 do artigo 5.º do RGPD, e consiste no cumprimento, por parte do responsável pelo tratamento, de todos os princípios anteriormente expostos, bem como na capacidade que este tem de comprovar que desempenhou as suas funções de acordo com os mesmos (n.º 1 do art. 24.º do RGPD). O responsável fica assim encarregue de estabelecer uma série de medidas técnicas e organizativas⁹³ que lhe permitam cumprir o disposto no n.º 1 do artigo 5.º do RGPD^{94, 95}.

Relativamente à parte final do n.º 2 do artigo 5.º do RGPD, esta é uma novidade introduzida pelo Regulamento, uma vez que não fazia parte do texto original do n.º 2 do artigo 5.º da Diretiva n.º 95/46/CE. Assim, e no que toca ao dever de comprovar o cumprimento do RGPD, temos duas opiniões divergentes: para A. Barreto Menezes Cordeiro, este dever “(...) *não consubstancia uma inversão do ónus da prova*”⁹⁶; sendo

⁹² SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, pp. 32-33. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021.

⁹³ Ver exemplos de medidas apresentados pelo Grupo de Trabalho do Artigo 29.º - “*Parecer 3/2010 sobre o princípio da responsabilidade*”, adotado em 13 de Julho de 2010, pp. 11-12.

⁹⁴ Deve ainda ter-se em atenção que a obrigação do cumprimento dos princípios elencados no n.º 1 do art. 5.º do RGPD não recai apenas sobre o responsável pelo tratamento, uma vez que “(...) *tantos os subcontratantes, como as autoridades de controlo, como todas as demais entidades que lidem com dados pessoais estão obrigados a respeitar os princípios fundacionais do RGPD*”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 161-162.

⁹⁵ Diário da República Eletrónico (s.d.), “*Princípio da integridade e confidencialidade*”. Disponível em <https://dre.pt/dre/LinkLexionarioAntigo?termoId=143859891>, acessado a 29 de abril de 2021.

⁹⁶ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 162.

que para Nuno Saldanha, “*estamos perante uma verdadeira inversão do ónus da prova*”⁹⁷. Neste sentido seguimos a vertente de Menezes Cordeiro, pois como o mesmo afirma, caso o responsável pelo tratamento não consiga fazer prova do cumprimento do RGPD “*(...) apenas será responsabilizado incumprimento do dever de comprovar*”.⁹⁸

O princípio da responsabilidade culmina no artigo 24.º do RGPD, sob a epígrafe “*responsabilidade do responsável pelo tratamento*”, que no seu n.º 1 consagra que “*(...) o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento (...)*”. Podemos mesmo referir que o artigo assinalado remete, para artigos como 35.º (“*avaliação de impacto sobre a proteção de dados*”), 36.º (“*consulta prévia*”), 40.º (“*códigos de conduta*”) e 42.º (“*certificação*”) do RGPD.

O incumprimento do princípio da responsabilidade é considerado, uma contraordenação muito grave, nos termos do artigo 83.º, n.º 5, alínea a) do RGPD e do artigo 37.º, n.º 1, alínea a) da Lei n.º 58/2019, de 8 de agosto, sendo aplicada a coima respetiva à dimensão da entidade (artigo 37.º, n.º 2 da Lei n.º 58/2019).⁹⁹

3.3 Direitos dos titulares

O RGPD prevê ainda uma série de direitos, atribuídos aos titulares de dados, com o objetivo de garantir que estes não se encontram desprovidos de controlo sobre os seus dados. Com a entrada em vigor do atual RGPD, os direitos do titular dos dados ganharam uma nova importância, não só pela nova redação de alguns destes (que já se encontravam previstos na Diretiva n.º 95/46/CE, revogada pelo Regulamento), como pela introdução de novos direitos.

Como será possível verificar ao longo desta dissertação, e tal como refere Nuno Saldanha, “*a cada um destes direitos cabe uma obrigação, por parte do responsável pelo*

⁹⁷ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 49, Lisboa, FCA - Editora de Informática.

⁹⁸ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 162.

⁹⁹ Diário da República Eletrónico (s.d.), “*Princípio da responsabilidade (tratamento de dados pessoais)*”. Disponível em <https://dre.pt/dre/lexionario/termo/principio-responsabilidade-tratamento-dados-pessoais>, acedido a 18 de janeiro de 2022.

tratamento (...)”.¹⁰⁰ Deste modo, de seguida serão analisados os direitos dos titulares de dados, sendo estes apresentados pela ordem pela qual se encontram dispostos no RGPD.

3.3.1 Direito de acesso

O direito de acesso encontra-se consagrado no n.º 1 do artigo 15.º do RGPD, onde se pode ler que “*o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às (...)*” informações estatuídas nas alíneas a) a h) do mesmo artigo.¹⁰¹

Para que tenha acesso aos dados pessoais que lhe dizem respeito, o titular dos mesmos deve, em primeira instância, proceder ao envio do pedido de informação¹⁰² ao responsável pelo tratamento. O responsável pelo tratamento, após “*(...) verificar a identidade do titular dos dados que solicite acesso (...)*” (Considerando 64 do RGPD)¹⁰³, deve fornecer uma cópia dos dados pessoais¹⁰⁴, sem quaisquer custos ou contrapartidas (artigo 12.º, n.º 5 do RGPD). Deve ter-se em conta que o acesso à referida cópia nem sempre é efetuado a título gracioso, uma vez que nas situações em que sejam, por parte do titular, requeridas mais cópias, “*(...) o responsável pode exigir o pagamento de uma taxa razoável (...)*” (artigo 15.º, n.º 3 do RGPD).¹⁰⁵

¹⁰⁰ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 53, Lisboa, FCA - Editora de Informática.

¹⁰¹ É possível identificar uma ligação entre o direito à informação (estatuído nos art. 13.º e 14.º do RGPD) e a obrigação atribuída ao responsável pelo tratamento, ou seja, fornecer ao titular dos dados as informações a que o mesmo tenha direito de aceder, cumprindo as restantes normas elencadas nos restantes números do artigo 15.º do RGPD, ver SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 34. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021. Da mesma opinião é A. Barreto Menezes Cordeiro, que chega mesmo a afirmar que “*(...) o denominado direito de acesso corresponde ao mais comum e usual direito à informação (...)*”, cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 263.

¹⁰² Este pedido tem como finalidade comprovar a existência ou não de tratamento dos dados do titular (primeira parte do n.º 1 do art. 15.º do RGPD).

¹⁰³ BRANCO, Flávia Machado Castelo (2018), “*O Regulamento Geral sobre a Proteção de Dados: Direitos dos Utilizadores*” (Dissertação de Mestrado), Instituto Superior de Contabilidade e Administração de Coimbra, Coimbra, p. 28. Disponível em <https://comum.rcaap.pt/handle/10400.26/27829>, acessado a 04 de março de 2021.

¹⁰⁴ De acordo com o n.º 4 do artigo 15.º do RGPD, “*o direito de obter uma cópia (...) não prejudica os direitos e as liberdades de terceiros*”, incluindo, nos termos do Considerando 63 do RGPD, “*(...) o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software*”.

¹⁰⁵ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 263-265.

Em suma, e em comparação com a anterior redação, viabilizada pela Diretiva n.º 95/46/CE, podemos mesmo afirmar que esta nova redação garante ao direito de acesso uma “(...) aplicação muito mais vasta”.¹⁰⁶

3.3.2 Direito de retificação

O direito à retificação, também conhecido por direito de atualização, encontra-se atualmente consagrado no artigo 16.º do RGPD¹⁰⁷. Através da leitura do exposto no referido artigo é possível identificar duas vertentes distintas, ou seja, “(...) o direito de obter (...) a retificação de dados pessoais inexatos que lhe digam respeito (...)” e o “(...) direito a que os seus dados pessoais incompletos sejam completados (...)”, tendo em conta as finalidades do tratamento. Para que haja lugar à correção ou atualização de dados (inexatos ou incompletos, respetivamente), deve ser, por parte do titular dos dados, realizado o pedido nos termos do artigo 12.º do RGPD. Após receção do mesmo cabe ao responsável pelo tratamento retificar ou completar os dados pessoais do titular, sem demora injustificada¹⁰⁸.¹⁰⁹ Assiste-lhe ainda a obrigação de notificar cada destinatário a quem tenham sido transmitidos os dados da retificação de dados pessoais (artigo 19.º do RGPD).

Concordamos assim com as palavras de Patrícia Andreia Batista e Santos, que defende que o direito de retificação “(...) está associado ao princípio da exatidão”¹¹⁰,

¹⁰⁶ BRANCO, Flávia Machado Castelo (2018), “*O Regulamento Geral sobre a Proteção de Dados: Direitos dos Utilizadores*” (Dissertação de Mestrado), Instituto Superior de Contabilidade e Administração de Coimbra, Coimbra, p. 27. Disponível em <https://comum.rcaap.pt/handle/10400.26/27829>, acedido a 04 de março de 2021.

¹⁰⁷ A Diretiva n.º 95/46/CE, apenas fazia, na alínea b) do seu artigo 12.º, uma breve referência ao direito de retificação, “(...) não lhe sendo atribuída qualquer densificação ou delimitação”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 269.

¹⁰⁸ Ao contrário do que acontece com os dados a retificar pelo responsável pelo tratamento, o texto do art. 16.º do RGPD não atribui aos dados incompletos a necessidade de serem completados sem demora injustificada, sendo que, “(...) contudo, isso mesmo se exige (...) à luz de uma interpretação sistemática do preceito e por invocação do regime geral previsto no artigo 12.º”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 273.

¹⁰⁹ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 270-273.

¹¹⁰ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 36. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

tendo por base a exatidão e a atualização dos dados pessoais sempre que necessária (alínea d) do n.º 1 do artigo 5.º do RGPD).

Este direito encontra-se ainda ligado ao direito de acesso, no sentido em que o titular dos dados, para proceder à retificação ou atualização dos dados pessoais que lhe digam respeito, tem que ter tido, numa fase anterior, acesso aos dados pessoais que o responsável pelo tratamento tem na sua posse.¹¹¹

3.3.3 Direito ao apagamento

O direito ao apagamento encontra-se definido no artigo 17.º do RGPD¹¹², sob a epígrafe “*Direito ao apagamento dos dados («direito a ser esquecido»)*”, denominação pela qual também é muitas vezes retratado. Para A. Barreto Menezes Cordeiro, estamos na presença de dois direitos distintos, o direito ao apagamento e o direito ao esquecimento, que por sua vez se encontram estatuídos nos números 1 e 2 do referido artigo, respetivamente.¹¹³ Assim sendo, o titular dos dados “*(...) tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada (...)*”¹¹⁴ quando:

- os dados pessoais deixem de ser necessários para a finalidade para a qual foram obtidos;
- retire o seu consentimento;
- se oponha oposição ao tratamento;
- os dados pessoais forem tratados ilicitamente; os dados tiverem de ser apagados para cumprimento de uma obrigação jurídica;
- e/ou os dados forem recolhidos no contexto da oferta de serviços de sociedade da informação (alíneas a) a f) do n.º 1 do art. 17.º do RGPD).

¹¹¹ BRANCO, Flávia Machado Castelo (2018), “*O Regulamento Geral sobre a Proteção de Dados: Direitos dos Utilizadores*” (Dissertação de Mestrado), Instituto Superior de Contabilidade e Administração de Coimbra, Coimbra, pp. 31-32. Disponível em <https://comum.rcaap.pt/handle/10400.26/27829>, acedido a 04 de março de 2021.

¹¹² A Diretiva n.º 95/46/CE, apenas fazia, na alínea b) do seu artigo 12.º, uma breve referência ao direito ao apagamento.

¹¹³ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 274.

¹¹⁴ Como referido anteriormente “*a cada um destes direitos cabe uma obrigação, por parte do responsável pelo tratamento (...)*”, e o direito ao apagamento não é exceção. Posto isto, é obrigação do responsável pelo tratamento “*(...) apagar os dados pessoais, sem demora injustificada (...)*” (segunda parte do n.º 1 do art. 17.º do RGPD). SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 58-59, Lisboa, FCA - Editora de Informática.

No que diz respeito ao direito ao esquecimento, este, nos termos do n.º 2 do artigo 17.º do RGPD, consiste “(...) *no direito a exigir ao responsável pelo tratamento que informe os demais responsáveis de que o titular dos dados solicitou o apagamento das ligações para esses dados pessoais, bem como o apagamento de eventuais cópias ou reproduções*”, sendo que o titular pode ainda, nos termos do artigo 19.º do RGPD requerer informações sobre os destinatários aos quais tenham sido transmitidos dados pessoais que lhe digam respeito.¹¹⁵

Deve ainda ser tido em conta que o direito ao apagamento de dados pessoais não permite, na sua atual conceção, o apagamento de todos e quaisquer dados pessoais, tendo para isso sido identificadas, no n.º 3 do artigo 17.º do RGPD as situações em que se prevê uma limitação a este direito.

O direito ao apagamento tem sido um dos direitos, que mais tem estado no centro de diferentes situações mediáticas relacionadas com a proteção de dados pessoais. Uma forma de constatar esta afirmação são os inúmeros litígios entre autoridades de controlo e grandes multinacionais ligadas ao tratamento de dados pessoais, como é o caso da Google LLC. Neste contexto podemos utilizar como exemplo o Acórdão do Tribunal de Justiça (Grande Secção), Processo C-507/17, de 24 de setembro de 2019, litígio que opôs a “*Google LLC*” (sucessora da “*Google Inc.*”) à Comissão Nacional de Informática e Liberdade Francesa (CNIL).¹¹⁶ O referido acórdão teve origem num pedido de supressão de uma lista de resultados, uma vez que o mesmo tem direito de, junto dos motores de busca, pedir a “(...) *desassociação de hiperligações da lista de resultados apresentada após uma pesquisa feita pelo seu nome (de-listing)*”.¹¹⁷ Pedido ao qual a Google LLC deu cumprimento, mas não na sua totalidade¹¹⁸, tendo-lhe sido, pela CNIL, aplicada, nos

¹¹⁵ Este direito é, na ótica de A. Barreto Menezes Cordeiro, considerado como “(...) *um reconhecimento da insuficiência do apagamento dos dados (...) em face das especificidades da Internet*”, uma vez que “(...) *o simples facto de se apagar uma determinada informação de um sítio não significa que ele tenha sido apagado de toda a Internet*”. Ver CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 275-277.

¹¹⁶ Acórdão do Tribunal de Justiça (Grande Secção), Processo C-507/17, de 24 de setembro de 2019. Consultado a 22 de junho de 2021, retirado de https://curia.europa.eu/juris/document/document_print.jsf?docid=218105&text=&dir=&doclang=PT&part=1&occ=first&mode=DOC&pageIndex=0&cid=4245208#Footnote*.

¹¹⁷ Comissão Nacional de Proteção de Dados (s.d.), “*Direito ao apagamento dos dados*”. Disponível em <https://www.cnpd.pt/cidadãos/direitos/direito-ao-apagamento-dos-dados/>, acessado a 23 de junho de 2021.

¹¹⁸ A “*Google LLC*” procedeu à supressão de referências, tal como requerido pelo titular dos dados pessoais, mas não o fez em todas as extensões de um nome do domínio do seu motor de busca.

termos da alínea i) do n.º 1 do artigo 58.º e artigo 83.º do RGPD, uma coima de 100.000,00 euros.

Perante estes factos, consta das declarações finais deste acórdão que, de acordo com a alínea b) do artigo 14.º da Diretiva n.º 95/46/CE (atualmente revogada) e do n.º 1 do artigo 17.º do RGPD, o operador não é obrigado a efetuar a supressão de referências em todas as versões do seu motor de busca, devendo somente fazê-lo nas versões deste que correspondem aos Estados-Membros. O operador fica ainda obrigado “(...) *a tomar todas as medidas que estiverem à sua disposição para assegurar uma supressão de referências eficaz e completa. Isto inclui, nomeadamente, a técnica denominada «bloqueio geográfico», a partir de um endereço IP presumivelmente localizado num dos Estados-Membros (...), independentemente do nome do domínio utilizado pelo internauta que efetue a pesquisa*”.¹¹⁹

3.3.4 Direito à limitação do tratamento

Como já foi anteriormente exposto¹²⁰, por limitação do tratamento podemos depreender que é a “(...) *inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro*” (n.º 3 do artigo 4.º do RGPD).

O titular dos dados tem, nos termos do artigo 18.º, n.º 1 do RGPD, o direito a obter a limitação do tratamento, por parte do responsável pelo mesmo, quando:

- conteste a exatidão dos dados¹²¹;
- se trate de um tratamento ilícito;
- os dados pessoais já não sejam considerados necessários para os fins para os quais tenham sido recolhidos;
- e/ou tenha sido realizado um pedido de oposição ao tratamento (alíneas a) a d) do n.º 1 do artigo 18.º do RGPD).

¹¹⁹ Acórdão do Tribunal de Justiça (Grande Secção), Processo C-507/17, de 24 de setembro de 2019. Consultado a 22 de junho de 2021, retirado de https://curia.europa.eu/juris/document/document_print.jsf?docid=218105&text=&dir=&doclang=PT&part=1&occ=first&mode=DOC&pageIndex=0&cid=4245208#Footnote*.

¹²⁰ Ver página 14 desta Dissertação.

¹²¹ Verificando-se a limitação do tratamento durante o período de tempo necessário para, pelo responsável pelo tratamento, ser verificada a exatidão dos dados pessoais (alínea a) do n.º 1 do art. 18.º do RGPD).

Tal como referido no direito de retificação e no direito ao apagamento dos dados, cabe ao responsável pelo tratamento a notificação, a cada destinatário a quem os dados pessoais tenham sido transmitidos, da limitação do tratamento realizada em conformidade com os pressupostos acima descritos (artigo 19.º do RGPD). Esta não será a única notificação a realizar por parte do responsável pelo tratamento, uma vez que, nos termos do n.º 3 do artigo 18.º do RGPD, deve informar o titular dos dados, que tenha obtido a limitação, de que a mesma será anulada e irá prosseguir com o tratamento dos seus dados pessoais.

O n.º 2 do referido artigo acrescenta que nas situações em que o responsável pelo tratamento tenha procedido à limitação dos dados pessoais, os mesmos “(...) *só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro*”.

3.3.5 Direito à portabilidade

O direito à portabilidade é uma das novidades apresentadas pelo RGPD e encontra-se salvaguardado no corpo do seu artigo 20.º. Assim, “*o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento (...) e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir (...)*”, mas o mesmo só se verifica se, cumulativamente, “*o tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato (...)*”¹²² “*(...) no qual o titular dos dados é parte ou para a realização de diligências pré-contratuais a pedido do titular dos dados (...)*”¹²³ e “*o tratamento for realizado por meios automatizados*”¹²⁴. Neste sentido, o responsável pelo tratamento deve assim desenvolver formatos interoperáveis, de forma a facilitar e promover a portabilidade dos dados (Considerando 68 do RGPD).

¹²² Alínea a) do n.º 1 do art. 20.º do RGPD.

¹²³ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 289.

¹²⁴ Alínea b) do n.º 1 do art. 20.º do RGPD.

A introdução do direito à portabilidade tem como objetivo o reforço do controlo do titular sobre os seus dados pessoais e a promoção de uma nova economia digital, garantindo uma maior concorrência no mercado digital¹²⁵.¹²⁶

No contexto laboral, um trabalhador tem direito à portabilidade dos seus dados se o tratamento se basear num contrato no qual o titular dos dados é parte (alínea b) do n.º 1 do artigo 6.º do RGPD por remissão da alínea a) do n.º 2 do artigo 9.º do mesmo). Utilizando o exemplo utilizado pelo Grupo de Trabalho do Artigo 29.º, num contexto de recursos humanos existem operações de tratamento, como serviços de remuneração e indemnização e recrutamento interno, que, sendo efetuadas através de meios eletrónicos, garantem aos trabalhadores o gozo do direito à portabilidade (alínea b) do n.º 1 do artigo 20.º do RGPD).¹²⁷

Devemos ainda ressaltar que o exercício do direito à portabilidade, atribuído ao titular dos dados, não prejudica o exercício do direito ao apagamento, podendo mesmo exercê-los em simultâneo, excetuando-se as situações em que se verifique a necessidade do tratamento “(...) *para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento*” (n.º 3 do artigo 20.º do RGPD).

3.3.6 Direito de oposição

O direito de oposição encontra-se atualmente elencado no artigo 21.º do RGPD¹²⁸, e atribui ao titular dos dados a capacidade “(...) *de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições (...)*” (primeira parte do n.º

¹²⁵ Uma vez que “(...) *a impossibilidade de receber e de transmitir os dados tende a desincentivar os consumidores/titulares de dados a mudar de prestador de serviço*”, o direito à portabilidade obriga ao “(...) *desenvolvimento de novas técnicas de tratamento de dados (...)*” e, conseqüentemente, a uma maior concorrência do próprio mercado. Ver CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 292.

¹²⁶ FIDALGO, Vitor Palmela (2019), “*O Direito à Portabilidade de Dados Pessoais*”, Revista de Direito e Tecnologia, Volume 1, NO. 1. Retirado de <https://blook.pt/publications/publication/cec4178f8a58/>, acedido a 26 de junho de 2021.

¹²⁷ Grupo de Trabalho do Artigo 29.º - “*Orientações sobre o direito à portabilidade dos dados*”, adotada em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017, pp. 9-10.

¹²⁸ Anteriormente encontrava-se definido no art. 14.º da Diretiva n.º 95/46/CE.

1 do artigo 21.º do RGPD). Ou seja, pode o titular dos dados, a todo o tempo¹²⁹, invocar o direito de oposição desde que se verifique, cumulativamente, que os motivos relacionados com a sua situação particular o justifiquem e o tratamento seja: “(...) *necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública (...)*” (alínea e) do n.º 1 do artigo 6.º do RGPD); “(...) *necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros (...)*” (alínea f) do n.º 1 do artigo 6.º do RGPD) ou “(...) *quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento (...)*” (n.º 4 do artigo 6.º do RGPD). Neste sentido é-nos possível identificar que a principal diferença entre o texto da Diretiva e do RGPD, relativo a este direito, é a limitação do âmbito de aplicação do mesmo, uma vez que “(...) *os Estados-Membros não podem estender o direito de oposição a outras situações*” para além das acima previstas.

Após a receção e análise do pedido enviado pelo titular, “*o responsável pelo tratamento cessa o tratamento dos dados pessoais (...)*”, exceto nas situações em que este comprove¹³⁰ e “(...) *apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial*” (segunda parte do n.º1 do artigo 21.º do RGPD).¹³¹

O exercício deste direito pode ser complementado com um pedido de apagamento, apresentado pelo titular dos dados, nos termos do artigo 17.º, n.º 1, alínea c) do RGPD, ficando o responsável pelo tratamento obrigado a apagar os dados pessoais do titular.¹³²

¹²⁹ Desde que o tratamento ainda não tenha sido efetuado na sua totalidade, uma vez o direito de oposição não tem efeito retroativo, o titular apenas pode exercê-lo antes ou durante o tratamento efetuado pelo responsável, cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 302.

¹³⁰ No sentido em que recai sobre o responsável pelo tratamento o ónus da prova (Considerando 69 do RGPD) e “*em caso de dúvida prevalece a oposição do titular dos dados*”. Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 303.

¹³¹ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 300-303.

¹³² SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 35. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

3.3.7 Direito a não ser avaliado com base em tratamento automático

De acordo com o disposto no n.º 1 do artigo 22.º do RGPD, “*o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente (...)*”. Podemos utilizar como referência as práticas de recrutamento eletrónico sem qualquer intervenção humana, sendo este um dos exemplos explanados no Considerando 71 do RGPD. Uma vez que este tratamento é realizado através da “*(...) definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais (...)*”¹³³ e quando o mesmo produza efeitos jurídicos que digam respeito ao titular dos dados, deve o mesmo opor-se ao referido tratamento, podendo mesmo suceder-se à cessação do mesmo por parte do responsável. É neste sentido que Patrícia Andreia Batista e Santos refere, na sua Dissertação, que o direito a não ser avaliado com base em tratamento automático “*pode ser visto como um direito especial de oposição (...)*”, visto que “*(...) não se configura como um direito, mas sim como uma obrigação do responsável (...)*” pelo tratamento.¹³⁴

Todavia, o texto do artigo 22.º do RGPD refere ainda que se as decisões forem: necessárias para a celebração ou a execução de um contrato; autorizadas pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito ou baseadas no consentimento explícito do titular (alíneas a), b) e c) do n.º 2 do artigo 22.º do RGPD, respetivamente), torna-se impossível para o titular invocar este direito.¹³⁵

3.4 O Responsável pelo Tratamento e o Subcontratante

Como será possível verificar ao longo desta Dissertação, as figuras do responsável pelo tratamento e do subcontratante são várias vezes mencionadas, devido à importância

¹³³ A definição de perfis realizada nas práticas de recrutamento eletrónico sem qualquer intervenção humana tem como objetivo “*(...) avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados (...)*”, cfr. Considerando 71 do RGPD.

¹³⁴ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, pp. 35-36. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

¹³⁵ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 63, Lisboa, FCA - Editora de Informática.

da sua atuação na proteção de dados pessoais. Apesar destas possuírem diferentes graus de responsabilidade, ambas serão alvos de escrutínio ao longo deste ponto.

De uma forma muito resumida, podemos definir o responsável pelo tratamento¹³⁶ como “(...) *quem efetivamente controla os dados (...)*”¹³⁷, sendo-lhe atribuída uma série de obrigações ao longo do RGPD. A primeira dessas encontra-se elencada no n.º 2 do artigo 5.º do mesmo Regulamento, onde se pode ler que o responsável pelo tratamento é responsável pelo cumprimento dos princípios relativos ao tratamento de dados pessoais (definidos ao longo do n.º 1 do artigo 5.º do RGPD), tal como o ónus de comprovar o cumprimento desses mesmos princípios.¹³⁸

O responsável assume assim o princípio da responsabilidade¹³⁹, recaindo sobre ele uma série de obrigações.¹⁴⁰ Neste sentido, são obrigações do responsável pelo tratamento:

- A aplicação de medidas técnicas e organizativas que forem adequadas¹⁴¹ para assegurar e comprovar que o tratamento é realizado em *compliance* com o RGPD (artigo 24.º, n.º 1 do RGPD);
- A aplicação de políticas adequadas (artigo 24.º, n.º 2 do RGPD);
- A aplicação de medidas, “(...) *tanto no momento de definição de meio de tratamento como no momento do próprio tratamento, (...) destinadas a aplicar*

¹³⁶ Ver página 17 desta Dissertação.

¹³⁷ À exceção de pessoas singulares que procedem ao tratamento de dados pessoais, de terceiros, na vigência de “(...) *atividades exclusivamente pessoais ou domésticas (...)*”, cfr. SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 75, Lisboa, FCA - Editora de Informática.

¹³⁸ SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., p. 73, Lisboa, FCA - Editora de Informática.

¹³⁹ Ver página 26 desta Dissertação.

¹⁴⁰ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 40. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

¹⁴¹ A adequação das medidas técnicas e organizativas varia consoante “(...) *a probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados (...)*” (Considerando 76 do RGPD), que por sua vez é determinado “*tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados (...)*”. (n.º 1 do art. 24.º do RGPD). A atuação do responsável pelo tratamento, ou do subcontratante, consiste numa abordagem baseada no risco (*risk based approach*). Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 317-320. Riscos esses que “(...) *podem resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais (...)*” (Considerando 83 do RGPD), bem como danos de natureza económica ou social (Considerando 75 do RGPD). Ver SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., pp. 74-75, Lisboa, FCA - Editora de Informática.

*com eficácia os princípios da proteção de dados (...)” e proteger os direitos dos titulares dos dados (artigo 25.º, n.º 1 do RGPD) - *privacy by design*^{142,143}*

- A aplicação de medidas “(...) *para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento (...)*” (artigo 25.º, n.º 2 do RGPD) - *privacy by default*¹⁴⁴;
- O registo de todas as atividades de tratamento sob a sua responsabilidade, efetuado por escrito, incluindo formato eletrónico (n.º 1 e 3 do art. 30.º do RGPD)¹⁴⁵;
- A cooperação com a autoridade de controlo (artigo 31.º do RGPD);
- A aplicação de medidas técnicas¹⁴⁶ e organizativas adequadas para assegurar um nível de segurança adequado ao risco (n.º 1 do artigo 32.º do RGPD)¹⁴⁷;
- A notificação da autoridade de controlo no caso de violação de dados pessoais (n.º 1 do artigo 33.º do RGPD)¹⁴⁸;
- A comunicação, ao titular, de violação de dados pessoais que implique um elevado risco para os seus direitos e liberdades (n.º 1 do artigo 34.º do RGPD);
- Proceder a uma avaliação de impacto das operações de tratamento (n.º 1 do artigo 35.º do RGPD);

¹⁴² Comissão Europeia (s.d.), “*O que significa a proteção de dados «desde a conceção» e «por defeito»?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt, acessido a 29 de junho de 2021.

¹⁴³ A pseudonimização é uma das medidas a aplicar, sendo reconhecida, a título exemplificativo, no texto do n.º 1 do art. 25.º do RGPD. Ver página 16 desta Dissertação.

¹⁴⁴ Comissão Europeia (s.d.), “*O que significa a proteção de dados «desde a conceção» e «por defeito»?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt, acessido a 29 de junho de 2021.

¹⁴⁵ Esta obrigação “(...) *não se aplica às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento seja suscetível de implicar um risco para os direitos e liberdades do titular, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.º*” (n.º 5 do artigo 30.º do RGPD).

¹⁴⁶ Apresentadas nas alíneas a) a d) do n.º 1 do art. 32.º do RGPD.

¹⁴⁷ O texto consagrado no n.º 1 do art. 32.º do RGPD “(...) *pode ser apresentado como uma manifestação (...) dos princípios da integridade e confidencialidade*”. Este não é o único princípio constante deste artigo, uma vez que, tal como se verifica no art. 25.º do RGPD, o princípio da proporcionalidade tem um papel importante na adequação das medidas “*tendo em conta as técnicas mais avançadas, os custos e aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares (...)*” (n.º 1 do art. 32.º do RGPD). Cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 346-347.

¹⁴⁸ Esta notificação pode ser efetuada através do preenchimento do Formulário de Violação de dados, disponível no site da CNPD. Disponível em <https://www.cnpd.pt/organizacoes/obrigacoes/>, acessido a 01 de julho de 2021.

Implementação do RGPD no Setor Empresarial

- Proceder à consulta prévia “(...) *quando a avaliação de impacto (...) indicar que o tratamento resultaria num elevado risco (...)*” (n.º 1 do artigo 36.º do RGPD);
- A designação de um encarregado de proteção de dados¹⁴⁹, também identificado como *data protection officer* (DPO) (n.º 1 do artigo 37.º do RGPD);
- A adoção, quando possível, de códigos de conduta (n.º 2 do artigo 40.º do RGPD);
- A adoção, quando possível, de procedimentos de certificação (n.º 1 do artigo 42.º do RGPD).

O responsável pelo tratamento pode, nos termos do artigo 28.º do RGPD, recorrer a um subcontratante, com o objetivo de que seja este a proceder ao tratamento de dados pessoais no seu lugar. Como já foi referido anteriormente, o subcontratante é considerado um mandatário do responsável pelo tratamento. De acordo com o n.º 3 do mesmo artigo do RGPD, o tratamento efetuado pelo subcontratante carece de regulamentação, podendo esta ser efetuada através de contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros. O objetivo desta materialização é a vinculação do subcontratante ao responsável pelo tratamento, bem como a estipulação de diversos elementos¹⁵⁰, como a limitação do tratamento “(...) *mediante instruções documentadas do responsável pelo tratamento (...)*”, a aplicação de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco (alíneas a) e c) do n.º 3 do artigo 28.º do RGPD, respetivamente), entre outros. Deve constar ainda deste contrato “(...) *o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento*”.

O controle da sua atuação fica a cargo do responsável pelo tratamento, de forma a garantir que o subcontratante a atua em prol da satisfação dos requisitos impostos pelo RGPD, assegurar a defesa dos direitos do titular dos dados (n.º 1 do artigo 28.º do RGPD) e a não violar as obrigações pelo qual é abrangido¹⁵¹.

¹⁴⁹ Esta figura tem uma importância a destacar no que diz respeito à implementação do RGPD

¹⁵⁰ Elencados nas alíneas a) a h) do n.º 3 do art. 28.º do RGPD.

¹⁵¹ O subcontratante partilha das mesmas obrigações que o responsável pelo tratamento de dados pessoais, sendo que algumas destas foram introduzidas com a entrada em vigor do Regulamento (UE) 2016/679, de 27 de abril de 2016.

De acordo com o n.º 2 do artigo 28.º do RGPD, o subcontratante pode “(...) *subcontratar o serviço, ou parte dele (...)*”¹⁵², carecendo de autorização por parte do responsável pelo tratamento.

Existem ainda situações¹⁵³ em que o tratamento de dados pessoais é realizado por um ou mais responsáveis, estando assim na presença de um tratamento conjunto. Os responsáveis determinam, entre eles e através de um acordo¹⁵⁴ escrito, “(...) *as respetivas responsabilidades pelo cumprimento do presente regulamento (...)*” (n.º 1 do artigo 26.º do RGPD), as suas funções e as relações entre si (n.º 2 do artigo 26.º do RGPD)¹⁵⁵. Podemos acrescentar ainda que, independentemente das disposições acordadas pelos diversos responsáveis, o titular dos dados pode exercer todos os direitos que lhe são atribuídos pelo RGPD em relação a cada um dos responsáveis pelo tratamento (n.º 3 do art. 26.º do RGPD).

3.5 Avaliação de Impacto sobre a Proteção de Dados

O artigo 35.º do RGPD¹⁵⁶ introduz a necessidade de o responsável pelo tratamento, antes da realização de operações de tratamento de dados pessoais, efetuar uma avaliação de impacto das operações previstas, também denominada de avaliação de impacto sobre a proteção de dados (AIPD). Essa avaliação incide, em particular, nas operações que utilizem novas tecnologias, “(...) *tendo em conta a sua natureza, âmbito, contexto e finalidades (...)*”, das quais possam resultar riscos para os direitos e liberdades dos titulares dos dados (n.º 1 do artigo 35.º do RGPD). A realização destas avaliações tem como principal objetivo evitar o incumprimento de normas dispostas do RGPD, mantendo assim a atuação do responsável pelo tratamento, em conformidade com as mesmas.¹⁵⁷

¹⁵² SALDANHA, Nuno (2018), “Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?”, s.e., p. 79, Lisboa, FCA - Editora de Informática.

¹⁵³ Por exemplo, quando “(...) *uma base de dados é comum a mais do que uma organização e partilhada*”, cfr. *Idem*, p. 75.

¹⁵⁴ Acordo este que não deverá ser disponibilizado ao titular dos dados, apenas a essência do mesmo (parte final do n.º 2 do art. 26.º do RGPD).

¹⁵⁵ No sentido em que “*não é necessário que todos os responsáveis contribuam com a mesma intensidade*”, cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 312.

¹⁵⁶ Considerandos 90 e 93 do RGPD.

¹⁵⁷ “*Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade*”, cfr. Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*”, revistas e adotadas pela última vez em 4 de outubro de 2017, p. 4.

A realização destas avaliações é obrigatória nas situações em que haja lugar: à “*avaliação sistemática e completa dos aspetos pessoais (...) baseada no tratamento automatizado, incluindo a definição de perfis (...)*” (alínea a) do n.º 3 do artigo 35.º do RGPD); a “*(...) operações de tratamento em grande escala de categorias especiais de dados (...) ou de dados pessoais relacionados com condenações penais e infrações*” (alínea b) do n.º 3 do artigo 35.º do RGPD); ou exista um “*controlo sistemático de zonas acessíveis ao público em grande escala*” (alínea c) do n.º 3 do artigo 35.º do RGPD). No entanto, devemos ter em conta que apesar da obrigatoriedade da realização da avaliação de impacto nas situações acima transcritas, existem outras das quais resulta risco tal para os titulares dos dados, que devem ser também sujeitas a avaliação de impacto sobre o tratamento de dados.¹⁵⁸ A título de exemplo, podemos considerar uma situação de controlo dos empregados, no que diz respeito à utilização de dispositivos da empresa, como uma situação da qual resulta a necessidade de realizar uma AIPD.¹⁵⁹

A avaliação de impacto sobre a proteção de dados inclui: uma descrição das operações de tratamento e a finalidade das mesmas; uma avaliação da necessidade e proporcionalidade; uma avaliação dos riscos para os direitos e para as liberdade dos titulares dos dados; bem como as medidas previstas para contornar os riscos associados a essas operações, incluindo garantias, medidas de segurança e procedimentos a utilizar com vista à proteção dos titulares dos dados e dos direitos inerentes a estes (alíneas a) a d) do n.º 7 do artigo 35.º do RGPD).

Nos casos em que da AIPD, resultem riscos elevados para a proteção de dados dos titulares dos mesmos, cabe ao responsável pelo tratamento a obrigação de consultar, antes de dar início às operações de tratamento, a autoridade de controlo, nos termos do artigo 36.º, n.º 1 do RGPD.¹⁶⁰

¹⁵⁸ *Idem*, p. 10.

¹⁵⁹ Tendo como critérios a existência de um controlo sistemático e o tratamento de dados relativos a titulares de dados vulneráveis, cfr. *Idem*, 13.

¹⁶⁰ Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*”, revistas e adotadas pela última vez em 4 de outubro de 2017, p. 21 & Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017, p. 10.

3.6 Autoridade de Controlo

O Regulamento (UE) 2016/679, de 27 de abril de 2016, prevê nos seus artigos 51.º e seguintes a existência de uma figura com responsabilidade de fiscalização da aplicação do mesmo, tendo em vista a defesa dos direitos e liberdades dos titulares dos dados (n.º 1 do art. 51.º do RGPD). Neste sentido, cabe a cada Estado-Membro estabelecer uma ou mais autoridades públicas, independentes, denominadas de autoridades de controlo¹⁶¹. A estas entidades são lhes atribuídos poderes de fiscalização, de correção, consultivos e de autorização (artigo 58.º, n.º 1, 2 e 3 do RGPD)¹⁶², bem como o poder de cooperação (artigo 60.º do RGPD), quando necessária, entre outras autoridades de controlo criadas por outros Estados-Membros ou até mesmo com a Comissão Europeia (Considerandos 117, 119 e artigo 51.º, n.º 2 do RGPD).

Em Portugal a autoridade de controlo competente pela aplicação coerente do RGPD é a Comissão Nacional de Proteção de Dados (CNPd)¹⁶³, “(...) *entidade administrativa independente, com personalidade jurídica de direito público e com poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto da Assembleia da República*”.¹⁶⁴

O regulamento faz ainda questão de, no seu artigo 52.º, identificar a principal característica afeta às autoridades de controlo, sendo essa, por sua vez, a independência com que estas agem na “(...) *prosecução das suas atribuições e no exercício dos poderes que lhe são atribuídos* (...)” (n.º 1 do referido artigo). Esta independência não pode ser afetada nem nas situações em que a autoridade de controlo fique sujeita a um controlo financeiro (Considerando 118 e art. 52.º, n.º 6 do RGPD).

Quanto à competência territorial destas autoridades, o RGPD prevê, no n.º 1 do seu artigo 55.º, que “*as autoridades de controlo são competentes para prosseguir as*

¹⁶¹ Ver página 19 desta Dissertação.

¹⁶² Comissão Europeia (s.d.), “*O que são autoridades de proteção de dados (APD)?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_pt, acessado a 07 de junho de 2021.

¹⁶³ Composto pela atual Presidente Maria Filipa Pires Urbano da Costa Calvão e mais seis membros, nos termos da Lei Orgânica da CNPD (Lei n.º 43/2004, de 18 de agosto) e dos art. 53.º e 54.º do RGPD. Comissão Nacional de Proteção de Dados (s.d.), “*O que somos e quem somos*”. Disponível em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>, acessado a 07 de junho de 2021.

¹⁶⁴ Comissão Nacional de Proteção de Dados (s.d.), “*O que somos e quem somos*”. Disponível em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>, acessado a 07 de junho de 2021.

atribuições e exercer os poderes que lhes são conferidos (...) no território do seu próprio Estado-Membro”.

Para além dos poderes previstos no artigo 58.º do RGPD, no artigo imediatamente anterior (artigo 57.º do RGPD), encontram-se estatuídas diversas funções e competências das autoridades de controlo, sendo estas:

- O controlo e execução do RGPD (alínea a) do n.º 1 do referido artigo);
- A promoção da sensibilização do público, quanto aos riscos, às regras, às garantias e aos direitos associados ao tratamento, bem como dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações (alíneas b) e d) do n.º 1 do referido artigo, respetivamente);
- Aconselhar o Parlamento nacional, o Governo e de qualquer outra instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades dos titulares dos dados (alínea c) do n.º 1 do referido artigo);
- Prestar informações, quando lhe sejam solicitadas, “(...) a qualquer titular de dados sobre o exercício dos seus direitos (...)” (alínea e) do n.º 1 do referido artigo)¹⁶⁵;
- Tratar das reclamações apresentadas e investigar o conteúdo das mesmas, devendo informar o autor da reclamação¹⁶⁶ do andamento e do resultado da investigação, num prazo razoável, especialmente se se verificar a necessidade de proceder a operações de investigação ou de coordenação com outras autoridades de controlo (alínea f) do n.º 1 do referido artigo)¹⁶⁷;
- Cooperar com outras autoridades de controlo (alínea g) do n.º 1 do referido artigo);
- Conduzir investigações sobre a aplicação do RGPD (alínea h) do n.º 1 do referido artigo);

¹⁶⁵ Caso se verifique essa necessidade, a autoridade de controlo deve cooperar com as autoridades de controlo de outros Estados-Membros de forma a informar qualquer titular sobre o exercício dos direitos que lhe são atribuídos pelo RGPD (segunda parte da alínea e) do n.º 1 do referido artigo).

¹⁶⁶ Podendo este ser o titular dos dados ou um organismo, organização ou associação por este mandatada, nos termos do artigo 80.º do RGPD.

¹⁶⁷ Nos termos do n.º 2 do art. 80.º do RGPD, a apresentação de reclamações deve ser facilitada pelas autoridades de controlo através da disponibilização de formulários de reclamação. Estes, por sua vez, e de forma a garantirem um maior acesso, devem salvaguardar ao autor da reclamação a possibilidade do seu preenchimento de forma eletrónica ou através de qualquer outro meio de comunicação.

Implementação do RGPD no Setor Empresarial

- Acompanhar a evolução “(...) *das tecnologias da informação e das comunicações e das práticas comerciais*” e quaisquer outros factos que tenham incidência na temática da proteção de dados pessoais (alínea i) do n.º 1 do referido artigo);
- A adoção de cláusulas contratuais-tipo no conteúdo dos contratos realizados entre o responsável pelo tratamento e o subcontratante, ou para os contratos realizados entre dois subcontratantes (n.º 3 e 4 do artigo 28.º, respetivamente, por remissão do n.º 8 mesmo artigo), bem como para a transferência de dados pessoais¹⁶⁸ para um país terceiro ou uma organização internacional (alínea j) do n.º 1 do referido artigo);¹⁶⁹
- Elaborar e conservar “(...) *uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35.º, n.º 4*” do RGPD (alínea k) do n.º 1 do referido artigo);
- Orientar, por escrito, o responsável pelo tratamento ou o subcontratante, no que concerne às operações de tratamento, cumprindo os prazos elencados no artigo 36.º, n.º 2 do RGPD (alínea l) do n.º 1 do referido artigo);
- Promover a elaboração de códigos de conduta, dar parecer sobre eles e aprovar aqueles que, na sua constituição, garantias suficientes, nos termos do artigo 40.º, n.º 1 e 5.º do RGPD, respetivamente (alínea m) do n.º 1 do referido artigo);
- Incentivar o “(...) *estabelecimento de procedimentos de certificação de proteção de dados, de selos e marcas de proteção de dados (...)*”, bem como aprovar os critérios de certificação, nos termos do artigo 42.º, n.º 1 e 5.º do RGPD, respetivamente (alínea n) do n.º 1 do referido artigo);
- Proceder, quando haja necessidade para tal, a uma revisão periódica das certificações emitidas (alínea o) do n.º 1 do referido artigo);
- Redigir e publicar “(...) *os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.º e de um organismo de certificação nos termos do artigo 43.º*” (alínea p) do n.º 1 do referido artigo);

¹⁶⁸ Elencada no art. 46.º, n.º 1 do RGPD.

¹⁶⁹ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 45. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

Implementação do RGPD no Setor Empresarial

- Conduzir o processo de acreditação “(...) *de um organismo para monitorizar códigos de conduta nos termos do artigo 41.º e de um organismo de certificação nos termos do artigo 43.º*” (alínea q) do n.º 1 do referido artigo);
- Autorizar as cláusulas contratuais e disposições constantes do n.º 3 do artigo 46.º do RGPD, relativas a transferências de dados pessoais um país terceiro (alínea r) do n.º 1 do referido artigo);
- Aprovar as regras vinculativas aplicáveis às empresas¹⁷⁰ (alínea s) do n.º 1 do referido artigo);
- Contribuir para as atividades do Comité (alínea t) do n.º 1 do referido artigo);
- Conservar registos internos de violações do presente regulamento e das medidas tomadas no exercício dos seus poderes de correção, nos termos do artigo 58.º, n.º 2 do RGPD (alínea u) do n.º 1 do referido artigo); e
- Desempenhar quaisquer outras funções relacionadas com a proteção de dados pessoais (alínea v) do n.º 1 do referido artigo).

Tal como exposto anteriormente, o artigo 58.º do RGPD acrescenta ainda que as autoridades de controlo se encontram providas de poderes de investigação, de correção e consultivo e de autorização (n.º 1, 2 e 3 do referido artigo, respetivamente). O poder de investigação atribuído às autoridades de controlo consiste na ordenação de fornecimento de informação, por parte do responsável pelo tratamento, necessária ao desempenho das suas funções (alínea a), do n.º 1 do referido artigo), na realização de auditorias sobre a proteção de dados (alínea b), do n.º 1 do referido artigo), na revisão de certificações emitidas nos termos do artigo 42.º, n.º 7 do RGPD (alínea c), do n.º 1 do referido artigo), na notificação de alegadas violações (alínea d), do n.º 1 do referido artigo), na obtenção de acesso a todos os dados e a todas as informações de que necessite (alínea e), do n.º 1 do referido artigo), bem como na obtenção de acesso às instalações do responsável pelo tratamento, incluindo os equipamentos por este utilizados para a realização das operações de tratamento (alínea f), do n.º 1 do referido artigo).

No que diz respeito ao poder de correção, este traduz-se na possibilidade de advertir o responsável pelo tratamento, com o objetivo de evitar a violação das normas

¹⁷⁰ Epígrafe do art. 47.º do RGPD.

Implementação do RGPD no Setor Empresarial

do RGPD (alínea a), do n.º 2 do referido artigo), na possibilidade de repreender o responsável pelo tratamento, nas situações em que o mesmo tenha infringido as normas do RGPD (alínea b), do n.º 2 do referido artigo), na ordenação da satisfação dos pedidos de exercício de direitos, por parte dos titulares dos dados pessoais (alínea c), do n.º 2 do referido artigo), na ordenação da utilização de medidas adequadas às operações de tratamento (alínea d), do n.º 2 do referido artigo), na ordenação da comunicação de violações de dados, aos respetivos titulares (alínea e), do n.º 2 do referido artigo), na imposição, temporária ou definitiva, da realização de operações de tratamento, podendo mesmo consubstanciar na sua proibição (alínea f), do n.º 2 do referido artigo), na ordenação da retificação, do apagamento ou da limitação do tratamento de dados (alínea g), do n.º 2 do referido artigo), na retirada da certificação ou ordenação da sua retirada ao organismo de certificação (alínea h), do n.º 2 do referido artigo), no estabelecimento de coimas, nos termos do artigo 83.º do RGPD (alínea i), do n.º 2 do referido artigo), bem com o na ordenação da suspensão do envio dos dados para destinatários localizados em países terceiros ou organizações internacionais (alínea j), do n.º 2 do referido artigo).

Por último, os poderes consultivos e de autorização que revestem as autoridades de controlo, são constituídos pelo aconselhamento realizado quando consultadas pelo responsável pelo tratamento, mais concretamente a consulta prévia¹⁷¹ (alínea a), do n.º 3 do referido artigo), pela emissão de pareceres dirigidos ao Parlamento nacional, ao Governo, bem como a outras instituições ou organismos (alínea b), do n.º 3 do referido artigo), pela autorização do tratamento realizado por um responsável no exercício de uma missão de interesse público¹⁷² (alínea c), do n.º 3 do referido artigo), pela emissão de pareceres e pela aprovação de projetos de códigos de conduta¹⁷³ (alínea d), do n.º 3 do referido artigo), pela acreditação de organismos de certificação¹⁷⁴ (alínea e), do n.º 3 do referido artigo), pela emissão de certificações e pela aprovação dos critérios de certificação desses organismos¹⁷⁵ (alínea f), do n.º 3 do referido artigo), pela adoção de cláusulas-tipo de proteção de dados¹⁷⁶ (alínea g), do n.º 3 do referido artigo), pela autorização de cláusulas contratuais¹⁷⁷ (alínea h), do n.º 3 do referido artigo), pela

¹⁷¹ Art. 36.º do RGPD.

¹⁷² Art. 36.º, n.º 5 do RGPD.

¹⁷³ Art. 40.º, n.º 5 do RGPD.

¹⁷⁴ Art. 43.º do RGPD.

¹⁷⁵ Art. 42.º, n.º 5 do RGPD.

¹⁷⁶ Previstas nos artigos 28.º, n.º 8 e 46.º, n.º 2, alínea d) do RGPD.

¹⁷⁷ Previstas no artigo 46.º, n.º 3, alínea a) do RGPD.

Implementação do RGPD no Setor Empresarial

autorização de acordos administrativos¹⁷⁸ (alínea i), do n.º 3 do referido artigo), assim como pela aprovação de regras vinculativas aplicáveis às empresas¹⁷⁹ (alínea j), do n.º 3 do referido artigo).

¹⁷⁸ Previstos no artigo 46.º, n.º 3, alínea b) do RGPD.

¹⁷⁹ Art. 47.º do RGPD.

4 Tratamento de Dados Pessoais no Contexto Laboral

4.1 Enquadramento

O progresso tecnológico, que temos vindo a presenciar nas últimas décadas, tem tido um impacto significativo nas nossas vidas, de diversas formas e em diferentes áreas, sendo que o setor laboral não é exceção.¹⁸⁰ Neste sentido, fazemos nossas as palavras de Sérgio Coimbra Henriques e João Vares Luís, quando referem que as novas tecnologias e os avanços no domínio digital ofereceram e continuarão a oferecer às entidades empregadoras e aos respetivos trabalhadores, novas formas de prestação da sua atividade laboral, possibilitando a melhoria do seu desempenho ou até a opção de trabalhar a partir de casa (regime de teletrabalho)¹⁸¹.

São inúmeros os desafios impostos pela introdução e utilização das novas tecnologias de informação nos locais de trabalho. É, por isso, imperativa a necessidade de, em detalhe, aprimorar as situações das quais provêm esses desafios, de forma a garantir a proteção do direito à vida privada dos trabalhadores, bem como dos dados pessoais destes. Esta necessidade teve origem nas diversas ocasiões nas quais a ténue linha que separa a esfera privada do trabalhador da sua atividade profissional é constantemente transposta. Note-se que, no seio das empresas, estas dificuldades representam um maior desafio para os departamentos de recursos humanos, “(...) *quer pela quantidade de tratamentos de dados pessoais sob a sua responsabilidade, quer pela quantidade de mecanismos técnicos e processos organizativos que têm de ser implementados (...)*”¹⁸². Esta atribuição de responsabilidade às empresas (também denominada de *accountability*), veio substituir a obrigação de notificação de tratamento à CNPD¹⁸³, tendo o responsável que proceder à realização de operações de tratamento de

¹⁸⁰ Uma vez que “*a generalidade das pessoas passa uma quantidade considerável do seu tempo no local de trabalho ou, pelo menos, a desempenhar funções laborais*” cit. HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “*Anuário de Proteção de Dados*”, p. 15. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

¹⁸¹ Ver páginas 77 a 80 desta Dissertação.

¹⁸² ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 19.

¹⁸³ Positivada no artigo 27.º da Lei n.º 67/98, de 26 de Outubro.

dados pessoais por sua conta em risco, garantindo que o faz em conformidade com as mesmas, sob pena de aplicação de sanções.¹⁸⁴

Devemos, então, ter em especial atenção que, no que diz respeito ao tratamento de dados pessoais no contexto laboral, o RGPD, veio atribuir aos diversos Estados-Membros, na primeira parte do n.º 1 do seu artigo 88.º, a possibilidade e a capacidade destes estabelecerem, no seu ordenamento jurídico, normas de cariz mais específico que aquelas já constantes deste diploma. Além disso, acrescenta que tais normas devem ter como propósito “(...) *garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral (...)*”. O n.º 2 do referido artigo acrescenta ainda que essas normas devem incluir “(...) *medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho*”. O Regulamento abre, assim, portas a diferentes interpretações e aplicações, criando simultaneamente a necessidade de suprir essa mesma lacuna.

Por sua vez, no ordenamento jurídico português, o tratamento de dados pessoais nas relações laborais encontra-se positivado no texto do artigo 28.º da Lei n.º 58/2019, de 08 de agosto, onde é atribuído ao empregador¹⁸⁵ a possibilidade de proceder ao tratamento de “(...) *dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código de Trabalho e respetiva legislação complementar ou noutros regimes setoriais (...)*”¹⁸⁶. No que diz respeito aos limites imposto pelo Código de Trabalho, referimo-nos às normas constantes dos artigos 16.º a 22.º desse mesmo Código¹⁸⁷. Normas essas, que dão forma à defesa dos direitos fundamentais de personalidade, privacidade e à reserva da intimidade da vida privada dos trabalhadores.

¹⁸⁴ HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “*Anuário de Proteção de Dados*”, pp. 14-18. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acedido a 20 de dezembro de 2021.

¹⁸⁵ A possibilidade de proceder ao tratamento de dados pessoais, atribuída ao empregador, é também atribuída a subcontratante ou a contabilista certificado, desde que realizado em nome do empregador (n.º 2 do art. 28.º, n.º 1 da Lei n.º 58/2019).

¹⁸⁶ Art. 28.º, n.º 1 da Lei n.º 58/2019, de 08 de agosto.

¹⁸⁷ Ver páginas 9 a 10 desta Dissertação.

Implementação do RGPD no Setor Empresarial

Do excerto do artigo 28.º da Lei n.º 58/2019, anteriormente transcrito, devemos ressaltar outro conceito de elevada importância: a finalidade para qual se procede ao tratamento de dados. Uma vez que, os dados pessoais só podem ser recolhidos para finalidades determinadas, explícitas e legítimas (artigo 5.º, n.º 1, alínea b) do RGPD)¹⁸⁸, é necessário compreender quais os fins que justificam a realização de operações de tratamento. Para tal, é imperativa a análise conjunta: do anteriormente mencionado n.º 1 do artigo 88.º do RGPD e do disposto na página 11 do Parecer 2/2017 do Grupo de Trabalho do Artigo 29.^{o189}. Desta interpretação, é-nos possível enunciar uma série de finalidades¹⁹⁰, perante as quais é exequível o tratamento de dados pessoais no contexto laboral, nomeadamente:

- o processo de recrutamento;
- a execução do contrato de trabalho (como por exemplo a gestão, planeamento e organização do trabalho; a igualdade e diversidade no local de trabalho; a saúde e segurança no trabalho; a proteção dos bens do empregador ou do cliente; e o exercício e gozo dos direitos e benefícios relacionados com o emprego); e
- a cessação da relação de trabalho.

Neste sentido, podemos constatar que as operações de tratamento de dados pessoais realizadas no contexto laboral não resultam, na sua totalidade, da execução do contrato de trabalho, nem apenas para o cumprimento de obrigações legais do empregador, uma vez que há lugar a operações de tratamento de dados pessoais mesmo antes de se verificar a existência de um vínculo laboral definitivo.¹⁹¹

¹⁸⁸ Definição que teve origem no texto do art. 6.º, n.º 1, alínea b) da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, dando lugar à utilização do Parecer 3/2013 sobre a limitação da finalidade, do Grupo de Trabalho do Artigo 29.º, com as devidas atualizações.

¹⁸⁹ O Parecer sobre o tratamento de dados no local de trabalho, que veio colmatar as falhas provocadas pela rápida evolução tecnológica e conseqüente desatualização de anteriores publicações do Grupo de Trabalho do Artigo 29.º, teve ainda como objetivo fazer “(...) *uma nova avaliação do equilíbrio entre o interesse legítimo dos empregadores e a expectativa razoável de privacidade dos empregados, sublinhando os riscos colocados pelas novas tecnologias e realizando uma avaliação da proporcionalidade de vários cenários em que poderiam ser aplicadas.*” cfr. Grupo de Trabalho do Artigo 29.º - “Parecer 2/2017 sobre o tratamento de dados no local de trabalho”, adotado em 8 de Junho de 2017, p. 4.

¹⁹⁰ Ver também ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, pp. 19-20.

¹⁹¹ NASCIMENTO, Ricardo & GAMA, Alexandre (2019), “*RGPD em Contexto Laboral*”, “*Boletim da Ordem dos Advogados*”, N.º 24 Setembro 2019, pp. 12-14. Disponível em <https://portal.oa.pt/publicacoes/boletim/edicoes-de-2019/edicoes-pdf-para-download/>, acedido a 10 de agosto de 2021.

De forma a sintetizar as temáticas abordadas ao longo deste enquadramento, devemos ter em conta que as operações de tratamento com vista a atingir as finalidades anteriormente mencionadas, carecem de regras e normas específicas, que, por sua vez, terão o seu devido destaque ao longo dos pontos seguintes. Numa primeira fase, e de forma a garantir a conformidade com as normas impostas pelo RGPD, é necessário compreender quais os fundamentos de licitude do tratamento de dados pessoais no contexto laboral.

4.2 Os Fundamentos de Licitude de Tratamento de Dados

Como já foi anteriormente referido nesta Dissertação, consta do art. 5.º, n.º 1, alínea a) do RGPD que os dados pessoais são “*objeto de um tratamento lícito, leal e transparente (...)*”, sendo por isso necessário verificar-se pelo menos uma das situações elencadas nas alíneas do n.º 1 do artigo 6.º do RGPD. No que ao tratamento de dados pessoais no contexto laboral diz respeito, devemos considerar como fundamentos de licitude as operações de tratamentos necessárias para: a execução de um contrato; o cumprimento de uma obrigação jurídica; e para efeitos de interesses legítimos do responsável pelo tratamento (alíneas b), c) e f) do n.º 1 do artigo 6.º do RGPD¹⁹², respetivamente).

Neste sentido, na alínea b) do artigo acima identificado, é possível ler-se que o tratamento de dados pessoais só é considerado lícito, se se verificar a sua necessidade para a execução de um contrato (do qual o titular dos dados seja parte integrante) ou para diligências pré-contratuais caso o pedido tenha sido por ele efetuado.¹⁹³ Podemos assim, a título exemplificativo, referir que o tratamento de dados realizado com vista ao pagamento da retribuição mensal dos trabalhadores, como exemplo de tratamento

¹⁹² Uma vez que o texto destes três fundamentos compreende a expressão “*necessário*”, devemos ter em conta as palavras de A. Barreto Menezes Cordeiro quando refere que “*o requisito da necessidade volta a assumir um preenchimento mais prático o que afasta da esfera de influência do princípio da proporcionalidade*”. Ver CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, pp. 205-206.

¹⁹³ Por outras palavras, devemos considerar lícito o tratamento de dados pessoais realizado desde o recrutamento efetuado pela entidade empregadora até à cessação do contrato de trabalho. Ver ainda, NASCIMENTO, Ricardo & GAMA, Alexandre (2019), “*RGPD em Contexto Laboral*”, “*Boletim da Ordem dos Advogados*”, N.º 24 Setembro 2019, p. 14. Disponível em <https://portal.oa.pt/publicacoes/boletim/edicoes-de-2019/edicoes-pdf-para-download/>, acedido a 10 de agosto de 2021.

Implementação do RGPD no Setor Empresarial

necessário para a execução do contrato de trabalho.¹⁹⁴ Ressalve-se que, este fundamento, de entre os analisados nos parágrafos seguintes, corresponde ao fundamento de licitude mais importante no contexto laboral, no sentido em que abrange um maior número de situações.

Para além do fundamento anteriormente mencionado, devemos considerar lícito o tratamento de dados “(...) *necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito*” (alínea c) do n.º 1 do artigo 6.º do RGPD). Neste seguimento, são obrigações jurídicas todas as obrigações legais impostas pelo direito laboral ao responsável pelo tratamento que, por sua vez, resultem na necessidade de proceder a operações de tratamento de dados pessoais dos trabalhadores¹⁹⁵. Podemos utilizar como exemplos de obrigações jurídicas do empregador: a comunicação obrigatória da admissão de novos trabalhadores à Segurança Social¹⁹⁶; o tratamento informático de dados referentes a filiação partidária dos trabalhadores (n.º 3 do artigo 457.º do CT)¹⁹⁷; o dever de manter o registo dos tempos de trabalho, incluindo dos trabalhadores que estão isentos de horário de trabalho (n.º 1 do artigo 202.º do CT)¹⁹⁸, entre outros.¹⁹⁹

Por último, tal como disposto no texto da alínea f) do n.º 1 do artigo 6.º do RGPD, é considerado lícito o tratamento “(...) *necessário para efeitos de interesses legítimos prosseguidos pelo responsável pelo tratamento* (...)”. Para que tal preceito seja

¹⁹⁴ Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017, p. 8.

¹⁹⁵ “*Sempre que o tratamento dos dados for realizado em conformidade com uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, (...) o tratamento deverá assentar no direito da União ou de um Estado-Membro (...)*”, cfr. Considerando 45 do RGPD.

¹⁹⁶ Que se deve reger pelas normas constantes “(...) *do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social, aprovado pela Lei n.º 110/2009, de 16 de setembro (...)*”, cfr. HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “*Anuário de Proteção de Dados*”, p. 29. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

¹⁹⁷ Os dados referentes à filiação sindical integram, nos termos do n.º 1 do art. 9.º do RGPD, as categorias especiais de dados, estando por isso o seu tratamento limitado. No entanto, a alínea b) do n.º 2 do referido artigo admite a possibilidade de tratamento desses dados no contexto laboral.

¹⁹⁸ Os registos dos tempos de trabalho devem ser mantidos “(...) *em local acessível e por forma a que permita a sua consulta imediata*” (n.º 1 do artigo 202.º do CT).

¹⁹⁹ Consultar estes e outros exemplos de obrigações jurídicas, no ordenamento jurídico português, em: HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “*Anuário de Proteção de Dados*”, pp. 29-30. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

considerando fundamento de licitude, é necessário que o interesse da entidade empregadora, para além de válido²⁰⁰, não se sobreponha aos direitos dos titulares dos dados, uma vez que, “(...) o tratamento de dados no local de trabalho deve ser realizado da forma menos intrusiva possível e ser dirigido para as áreas específicas de risco”²⁰¹. O responsável pelo tratamento deve então proceder à adoção e aplicação de “(...) métodos ou tecnologias específicas (...)”, de forma proporcional e adequada²⁰², com vista ao tratamento de dados pessoais, garantindo sempre um “(...) equilíbrio entre a prossecução de uma finalidade (legítima) de tratamento de dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores (...)”.²⁰³ Ressalve-se que, no caso de se verificar uma situação de desequilíbrio, da qual resulte a violação dos direitos do titular, o RGPD atribui a este a capacidade de se opor, a qualquer momento, ao tratamento dos seus dados, nos termos do n.º 1 do seu artigo 21.º.²⁰⁴ No entanto, para que seja possível ao titular opor-se, a uma ou mais operações de tratamento, é necessário que, numa primeira fase, o mesmo tenha conhecimento da sua existência. De forma a garantir o acesso do trabalhador aos direitos que lhe são atribuídos pelo RGPD, o responsável pelo tratamento está obrigado a informar/dar conhecimento dessas operações.

O motivo de interesse legítimo mais comumente invocado pelas entidades empregadoras é o aumento da produtividade, abrindo portas a diversas situações das quais resulta a necessidade de proceder a operações de tratamento de dados. Podemos utilizar, como exemplo: a utilização de sistemas para a monitorização dos tempos de trabalho, através do controlo de pontualidade e de assiduidade dos funcionários (que será abordada mais à frente nesta Dissertação). Deste controlo, resulta o tratamento de dados biométricos dos trabalhadores dessa empresa, independentemente das suas funções. Deve, então, verificar-se uma harmonia entre as medidas adotadas e os direitos dos titulares dos dados. A limitação das finalidades do tratamento é um dos métodos que tem como intuito a referida harmonia. Os dados pessoais tratados através de sistemas de

²⁰⁰ Ver páginas 22 a 23 desta Dissertação.

²⁰¹ Grupo de Trabalho do Artigo 29.º - “Parecer 2/2017 sobre o tratamento de dados no local de trabalho”, adotado em 8 de Junho de 2017, p. 9.

²⁰² Grupo de Trabalho do Artigo 29.º - “Parecer 2/2017 sobre o tratamento de dados no local de trabalho”, adotado em 8 de Junho de 2017, p. 9.

²⁰³ HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “Anuário de Proteção de Dados”, p. 31. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

²⁰⁴ Ver páginas 34 a 25 desta Dissertação.

controlo de pontualidade e assiduidade, com vista ao aumento da produtividade, não podem ser utilizados, “(...) *como elemento de avaliação dos (...)*” trabalhadores.²⁰⁵ Acrescentamos ainda, que o referido controlo, para além de ser considerado interesse legítimo desta entidade é também uma obrigação jurídica resultante do artigo 202.º do CT.

Recapitulando, podemos constatar que no contexto laboral a entidade empregadora tem à sua disposição três fundamentos invocáveis, perante os quais é lícito o tratamento de dados pessoais dos seus trabalhadores. Existe ainda a possibilidade de se verificar a aplicação de mais do que um desses fundamentos em simultâneo.

Neste sentido, podemos levantar a seguinte questão:

Porque é que o consentimento do titular dos dados (alínea a), do n.º 1 do artigo 6.º do RGPD), não é considerado um fundamento de licitude do tratamento de dados pessoais realizado pela entidade empregadora?

O consentimento é, nos termos do n.º 11 do artigo 4.º do RGPD, “(...) *uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita (...) que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*”.²⁰⁶ Essa manifestação deve ser efetuada através de uma declaração, escrita, ou ato positivo inequívoco. Para além disso, importa ainda referir que, o consentimento é, nos termos da alínea a) do n.º 1 do artigo 6.º do RGPD, um fundamento de licitude do tratamento, chegando mesmo a ser conotado “(...) *como a principal causa de legitimidade e de licitude do tratamento de dados pessoais*”^{207, 208}.

²⁰⁵ HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, “*Anuário de Proteção de Dados*”, pp. 32-34. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

²⁰⁶ Ver páginas 18 desta Dissertação.

²⁰⁷ Podemos considerar que esta afirmação colide, com o destaque por nós efetuado aquando da análise da execução de um contrato como fundamento de licitude no contexto laboral (nas páginas 51 a 57 desta Dissertação). Ambos os fundamentos de licitude, apresentados pelo artigo 6.º do RGPD, são considerados os mais importantes. Note-se, então, que existe uma diferença, que apesar de pequena não é, de forma alguma, insignificante. Referimo-nos ao contexto em que o fundamento é aplicado, ou seja, a situação em que se verifica a necessidade de consentimento para a realização de operações de tratamento de dados. Neste caso, o contexto laboral.

²⁰⁸ CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 167.

Porém, não é considerado um fundamento de licitude no contexto laboral, uma vez que existe uma subordinação do trabalhador perante a entidade empregadora²⁰⁹ (o contrato de trabalho). O Parecer 2/2017 do Grupo de Trabalho do Artigo 29.º, acrescenta ainda que “(...) *quando um empregador tenha de proceder ao tratamento de dados pessoais dos seus empregados, é enganoso partir da suposição de que o tratamento pode ser legitimado através do consentimento dos empregados*”. Vejamos, se o titular dos dados não dispuser de uma escolha verdadeira ou livre, ou se de alguma forma o mesmo não possuir a capacidade de recusar nem retirar o seu consentimento sem ser prejudicado, não podemos considerar que o consentimento tenha sido cedido livremente. Podemos, por outras palavras, afirmar que a decisão do mesmo foi tomada sob coação²¹⁰ (impedindo o titular dos dados de exercer livremente a sua escolha)²¹¹, com medo e receio das consequências que poderiam daí advir, violando o disposto do n.º 3 do artigo 7.º do RGPD. Neste sentido, e uma vez que não se verifica a existência de consentimento nos termos da definição atribuída pelo n.º 11 do artigo 4.º do RGPD, não podemos considerar a validade do mesmo.²¹²

A existência de um contrato de trabalho entre as partes pressupõe uma dependência económica²¹³ e conseqüentemente “(...) *um desequilíbrio entre o titular dos dados e o responsável pelo seu tratamento (...)*” (Considerando 43 do RGPD). Podemos, assim, considerar que são escassas as ocasiões em que os trabalhadores possuem o livre-arbítrio para dar o seu consentimento. Nesta perspetiva, o RGPD veio introduzir a necessidade de avaliar: se o consentimento é ou não dado livremente. A avaliação tem como objetivo confirmar se “(...) *a execução de um contrato (...)* está subordinada ao

²⁰⁹ “*O que verdadeiramente caracteriza o contrato de trabalho é a subordinação jurídica que mais não é do que a dependência em que o trabalhador se encontra perante o empregador no que diz respeito à forma como deve prestar a sua atividade, estando obrigado a obedecer às ordens e instruções que aquele venha a emanar, dentro dos limites do contrato e das normas que o regem*”, cfr. Procuradoria-Geral Distrital de Lisboa (s.d.), “*Sumários do STJ (Boletim) - Laboral*”, “*ACSTJ de 08-02-2006*”. Disponível em http://www.pgdlisboa.pt/jurel/stj_mostra_doc.php?nid=22142&codarea=3, acessado a 17 de janeiro de 2022.

²¹⁰ Artigo 256.º e 255.º do Código Civil, respeitantes à “*falta de consciência da declaração e coação física*” e à “*coação moral*”, respetivamente.

²¹¹ “*Todos os condicionamentos à liberdade do titular dos dados devem ser considerados*”, cfr. CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina, p. 174.

²¹² Grupo de Trabalho do Artigo 29.º - “*Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*”, adotado em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018, pp. 7-8.

²¹³ Uma vez que o “*contrato de trabalho é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua atividade a outra pessoa (...)*” (art. 11.º do CT).

Implementação do RGPD no Setor Empresarial

consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato” (n.º 4 do artigo 7.º do RGPD).

No que diz respeito à aplicação desta limitação no ordenamento jurídico português, o n.º 3 do artigo 28.º da Lei n.º 58/2019, de 08 de agosto, introduz a impossibilidade de o consentimento ser considerado requisito de legitimidade, se “*o tratamento for necessário para a execução de um contrato do qual o titular é parte (...)*” (alínea b) do n.º 1 do artigo 6.º do RGPD)²¹⁴. No entanto, podemos ponderar a existência de situações em que o tratamento de dados pessoais de um trabalhador, com base no consentimento é lícito, sobretudo se tal tratamento for do interesse do mesmo²¹⁵. Veja-se, a título de exemplo, uma situação em que uma empresa conceba “*(...) benefícios ao trabalhador ou aos familiares deste (por exemplo, descontos nos serviços da empresa (...))*”²¹⁶.

Com a entrada em vigor do RGPD, a entidade empregadora tem a obrigação de informar, novamente, os seus trabalhadores, relativamente aos direitos que lhes são atribuídos, independentemente de a recolha dos dados pessoais ter sido realizada junto, ou não, do titular dos mesmos (nos termos do artigo 13.º e 14.º do RGPD). Das informações que a entidade empregadora deve prestar aos titulares dos dados, devem constar ainda quais os seus dados sujeitos a tratamento, bem como as finalidades desse tratamento. Assim, e de forma a que seja possível verificar-se o *compliance* das medidas tomadas para com as normas constantes do RGPD, a entidade empregadora deve rever as políticas internas de tratamento de dados pessoais, efetuar aditamentos aos contratos de trabalho já existentes e implementar novas cláusulas de tratamento de dados pessoais nos contratos de trabalho futuros. Caso contrário, a falta de adoção de normas relativas às

²¹⁴ Alíneas a) e b) do n.º 3 do art. 28.º da Lei n.º 58/2019, respetivamente.

²¹⁵ Devemos ter especial atenção ao disposto na alínea a) do n.º 3 do art. 28.º da Lei n.º 58/2019, onde podemos ler que “*(...) o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador (...)*”. Não obstante, a Comissão Europeia, apresenta um exemplo em que o consentimento do titular é considerado fundamento de licitude do tratamento de dados, e este beneficia dessas mesmas operações, estamos na presença de um conflito de entendimentos. Neste sentido, a CNPD desaplicou a norma constante da alínea a) do n.º 3 do art. 28.º da Lei n.º 58/2019, através da Deliberação/2019/494 da CNPD. Cfr. ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 59.

²¹⁶ Comissão Europeia (s.d.), “*O meu empregador pode obrigar-me a dar consentimento para utilizar os meus dados?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_pt, acessado a 07 de janeiro de 2022.

obrigações legais da entidade empregadora, e consequente “(...) violação das disposições referentes (...) aos princípios básicos do tratamento ou aos direitos dos titulares (...)”, dará lugar à aplicação de coimas até aos 20.000.000,00€ (vinte milhões de euros), ou até 4% do seu volume anual de negócios a nível mundial (correspondente ao exercício financeiro anterior), consoante o montante que for mais elevado (n.º 5 do artigo 83.º do RGPD).

4.3 Processos de Recrutamento

4.3.1 Tratamento de Dados Pessoais

O processo de recrutamento, também conhecido por *talent acquisition*, é o processo pelo qual uma empresa procura um ou mais candidatos para o preenchimento de vagas e/ou criação de base de dados (com pretensão ao preenchimento de futuras vagas). Os trâmites deste procedimento são da competência dos departamentos de recursos humanos das diversas empresas.

Durante a pendência deste procedimento, são diversas as situações das quais advém a necessidade de realizar operações de tratamento de dados pessoais resultantes, principalmente, da procura ativa de emprego. Esta procura pode ser efetuada através da inscrição no Instituto do Emprego e Formação Profissional (IEFP), como através da iniciativa própria do candidato (em resposta a ofertas de emprego e através do envio de candidaturas espontâneas²¹⁷). Independentemente da modalidade escolhida, geralmente, dá-se por iniciado o processo de recrutamento aquando da receção da candidatura, em formato físico ou digital. O tipo de candidatura habitual passa pelo envio de um documento, mais comumente conhecido por currículo (CV), do qual devem constar informações relativas ao candidato, tais como: dados pessoais (nome, idade, e-mail, contacto telefónico, entre outros); formação; qualificações e experiência profissional; idiomas; entre outras. Não obstante deste, atualmente tem-se verificado um aumento

²¹⁷ No que diz respeito à procura ativa de emprego tem-se verificado um aumento do envio de candidaturas espontâneas, não só por parte de pessoas desempregadas, como também por pessoas empregadas e descontentes com as suas situações (muitas das vezes precárias).

notório de candidaturas submetidas através do preenchimento de formulários online, bem como da utilização de redes sociais profissionais (como por exemplo o *LinkedIn*²¹⁸).²¹⁹

Perante a receção do CV do candidato, e no seguimento do processo de recrutamento da empresa, seria normal, o departamento de recursos humanos iniciar, de forma imediata, a recolha e o tratamento dos dados constantes da candidatura. No entanto, com a introdução do RGPD, as empresas passam a estar obrigadas a obter o consentimento inequívoco dos candidatos (alínea a) do n.º 1 do artigo 6.º do RGPD).²²⁰ Este preceito veio eliminar a capacidade que o responsável pelo tratamento tinha de realizar operações de tratamento com base na presunção de consentimento do titular, apenas pela submissão da sua candidatura.²²¹ Cabe então aos departamentos de recursos humanos a criação de procedimentos para a obtenção do consentimento do titular dos dados, independentemente da forma como este procedeu à submissão da sua candidatura.²²² Deve assim, nos termos do Considerando 42 do RGPD, ser facultado ao titular dos dados, declaração, da qual consta a identificação do responsável pelo tratamento (alínea a) do n.º 1 do artigo 13.º do RGPD), a finalidade a que se destina (alíneas c) do n.º 1 do artigo 13.º do RGPD) e o prazo de conservação desses dados. A existência deste documento atribui ao responsável pelo tratamento a capacidade de comprovar que o “(...) *titular dos dados deu o seu consentimento para o tratamento dos seus dados (...)*” (n.º 1 do artigo 7.º e do Considerando 42, ambos do RGPD).

Ao contrário daquilo que foi referido anteriormente nesta Dissertação, no que diz respeito ao tratamento de dados pessoais realizado durante o processo de recrutamento, o consentimento é considerado legítimo. Não obstante, caso se verifique que o titular dos

²¹⁸ *LinkedIn* é uma rede social de negócios, resultado direto da evolução tecnológica, maioritariamente “(...) utilizada por profissionais com o intuito de apresentar suas aptidões (...)”, seja a possíveis e futuras entidades empregadoras, como a profissionais da mesma empresa, cfr. <https://pt.wikipedia.org/wiki/LinkedIn> (acedido a 01 de janeiro de 2022).

²¹⁹ O candidato que possua um perfil de uma rede social profissional deve incluir o endereço do seu perfil no seu currículo.

²²⁰ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 53.

²²¹ BAIRRÃO, Isabel (2019), “*Os dados dos seus colaboradores respeitam o RGPD?*”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acedido a 07 de janeiro de 2022.

²²² Ressalve-se que nas situações em que sejam submetidas candidaturas espontâneas, o cumprimento deste preceito implicará uma melhor organização e uma preparação prévia de declarações de consentimento, uma vez que será necessário manter os dados constantes da candidatura numa base de dados até à abertura de uma vaga. Ver: BAIRRÃO, Isabel (2019), “*Os dados dos seus colaboradores respeitam o RGPD?*”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acedido a 07 de janeiro de 2022.

dados não dispõe de uma escolha verdadeira ou livre, ou não puder recusar nem retirar o seu consentimento sem ser prejudicado, não estamos na presença de um consentimento válido (n.º 2 do artigo 7.º e alínea a) do n.º 1 do artigo 6.º, ambos do RGPD, respetivamente).

Para além das anteriormente analisadas, devemos ter em conta a existência de outra modalidade de recrutamento, denominada de recrutamento ativo. Esta modalidade consiste na procura e recrutamento de profissionais competentes para uma vaga específica, ou seja, o departamento dos recursos humanos entra diretamente em contacto com as pessoas que considera mais acertadas para a vaga em questão. Apesar de limitar a amplitude da procura de candidatos, e conseqüentemente, evitar a acumulação de candidaturas consideradas desnecessárias, também limita o acesso à informação dos mesmos. Por sua vez, este constrangimento no acesso às informações dos possíveis candidatos tem vindo a diminuir graças à existência de redes sociais profissionais, como o *LinkedIn*. Estas novas ferramentas, para além de representarem um espaço onde qualquer sujeito pode colocar informações relativas às suas qualificações e experiência profissional, bem como à sua formação (quase como que se de um cartão de visita se tratasse), acabam por permitir a separação da vida profissional da vida pessoal (constante de redes sociais como o *Facebook*, *Instagram*, entre outros). Contudo, continua a ser necessário o acesso a mais informações do candidato, devendo o responsável pelo tratamento solicitar o consentimento do mesmo, de forma a prosseguir com o tratamento dos seus dados pessoais.²²³

Mantendo a temática das redes sociais, mais concretamente no que diz respeito à separação da vida profissional, da pessoal, tem-se verificado um aumento de acessos, indiscriminados, a perfis públicos de candidatos com vista à obtenção de mais informações sobre os mesmos²²⁴. É espectável que quanto maior for a quantidade de informações sobre um candidato, mais fácil é reconhecer se o mesmo se adapta às necessidades da empresa, contudo, não é justificação para a invasão da esfera privada do candidato. Neste sentido, é necessário um fundamento jurídico, nomeadamente um interesse legítimo (alínea f) do n.º 1 do artigo 6.º do RGPD) para efetuar este tratamento,

²²³ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 54.

²²⁴ Através da consulta dos perfis sociais públicos, como é o caso do *Facebook*, *Instagram*, *Twitter*, entre outros.

devendo o responsável pelo tratamento, “(...) *antes da inspeção do perfil no meio social, ter em conta se o perfil no meio social do candidato diz respeito a fins profissionais ou privados (...)*”. Acresce ainda a obrigação de circunscrever a recolha e tratamento de dados pessoais, àqueles que digam respeito às funções que iriam desempenhar, caso fossem selecionados para a vaga para a qual se candidataram.²²⁵

Outra problemática resultante da evolução tecnológica, no que diz respeito ao processo de recrutamento, é a utilização de sistemas automatizados²²⁶ de apoio a estes processos, também conhecidos por *applicant tracking system* (ATS). A utilização desses sistemas tem como objetivo a avaliação de candidatos, através da definição de perfis (artigo 4.º, n.º 4 do RGPD)²²⁷. Atualmente, e de forma a atingir esse objetivo de forma mais célere, foram adotados e integrados nos sistemas automatizados de recrutamento, ferramentas de inteligência artificial, que recolhem dados pessoais “(...) *a partir de diferentes fontes públicas e privadas (...)*”.²²⁸ Apesar de prevista nos termos da alínea a) do n.º 2 do artigo 22.º do RGPD, devemos ter em especial atenção que, a utilização destas ferramentas no contexto do processo de recrutamento é uma exceção à regra, uma vez que o RGPD, no n.º 1 do seu artigo 22.º, atribui ao titular dos dados “(...) *o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado (...)*”. Porém, e não menos importante, o RGPD atribui ao titular o direito de acesso aos seus dados, bem como o direito a ser informado sobre o tratamento dos seus dados, mesmo quando os dados pessoais não tenham sido recolhidos junto deste (artigo 14.º do RGPD). Cabe, então, ao responsável pelo tratamento a responsabilidade de informar o titular dos dados da existência de operações de tratamento.²²⁹ Caso contrário, se mantiver as operações de tratamento em segredo, o responsável pelo tratamento incorre na violação das normas dispostas, no supramencionado, artigo 14.º do RGPD e

²²⁵ Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017, pp. 13-14.

²²⁶ De referir que a utilização de *softwares* começa a ser mais frequente também no controlo dos tempos de trabalho, na avaliação de desempenho, entre outras situações do contexto laboral.

²²⁷ Ver páginas 14 a 16 desta Dissertação.

²²⁸ Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à transparência na aceção do Regulamento 2016/679*”, adotadas em 2 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018, pp. 6-8.

²²⁹ HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “*Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*”, “Anuário de Proteção de Dados”, p. 23. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessado a 20 de dezembro de 2021.

consequente aplicação de coimas nos termos da alínea b) do n.º 5 do artigo 83.º do RGPD.²³⁰

Por último, é necessário compreender o que fazer aos dados dos candidatos que, aquando do término do processo de recrutamento²³¹, acabaram por não ser recrutados. O departamento de recursos humanos deve, então, solicitar o consentimento do titular dos dados para que seja possível mantê-los em base de dados. Estas, por sua vez, têm como objetivo o armazenamento de dados de candidatos até à abertura de novas vagas.²³² Atente-se, no entanto, que no caso de se iniciar um novo processo de recrutamento, deve ser novamente solicitado o consentimento do titular dos dados. Neste contexto, da declaração de consentimento deve constar um, ou mais, finalidades, diferentes das que constavam da declaração de consentimento quando do armazenamento em base de dados.²³³ Estes preceitos são de igual forma aplicados nas situações em que forem submetidas candidaturas espontâneas, devendo estas ser armazenadas (caso o titular assim o consinta) até a abertura de novas vagas. Caso contrário, ou nas situações em que o titular manifeste a sua oposição ao tratamento²³⁴ de dados (nos termos do n.º 1 do artigo 21.º do RGPD) com vista ao armazenamento, todos os dados devem ser imediatamente eliminados²³⁵ (tenham estes sido recolhidos durante o processo de recrutamento ou através da submissão de candidaturas espontâneas).

Cabe-nos, agora, compreender durante quanto tempo devem e podem esses dados ser mantidos no domínio do responsável pelo tratamento.

²³⁰ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, pp. 54-55. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021.

²³¹ “*Todas as entidades devem manter durante cinco anos o registo dos processos de recrutamento efetuados (...)*” (n.º 1 do art. 32.º do CT).

²³² ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 53.

²³³ BAIRRÃO, Isabel (2019), “*Os dados dos seus colaboradores respeitam o RGPD?*”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acessado a 07 de janeiro de 2022.

²³⁴ Ver páginas 34 a 36 desta Dissertação.

²³⁵ Ver páginas 30 a 32 desta Dissertação.

4.3.2 Período de Conservação de Currículos

O Regulamento Geral sobre a Proteção de Dados, na sua constituição, apesar das várias menções ao prazo de conservação dos dados pessoais²³⁶, não chega a estabelecer nenhum prazo específico. Neste sentido, tal concretização ficaria, nos termos do n.º 1 do artigo 88.º do RGPD, a cargo da legislação portuguesa. Encontra-se disposto no n.º 1 do artigo 21.º da Lei n.º 58/2019, de 8 de agosto, que “*o prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade*”.

Não existindo um limite definido relativamente ao período de conservação dos currículos, cabe às próprias entidades estabelecer um prazo limite para o mesmo. Não devemos esquecer que a fixação deste prazo tem carácter de obrigatoriedade, uma vez que este é uma das informações a facultar ao titular nos termos dos artigos 13.º e 14.º do RGPD. Regra geral, o prazo de conservação utilizado pela maior parte das empresas em Portugal, é de um ano a contar da receção dos dados. Salienta-se, que a fixação deste prazo tem por base o entendimento da CNPD quando refere que “*(...) os dados de candidatos estarão desatualizados ao fim de um ano a contar da recolha*”.²³⁷ Verificamos assim a aplicação dos princípios da minimização e da exatidão, garantindo que apenas os dados são adequados e limitados, e que os mesmos se encontram atualizados (alíneas c) e d) do n.º 1 do artigo 5.º do RGPD, respetivamente).

Em comparação com os outros, é possível verificar que o prazo relativo à conservação de currículos é dos mais curtos. Sucede então que a fixação deste é inerente, entre outros pressupostos, à finalidade a que se destina, sendo que “*(...) na delimitação dos prazos de conservação é fundamental que sejam especificadas com rigor as finalidades e que as mesmas sejam do conhecimento dos titulares dos dados*”.²³⁸

Assim, e como havia sido anteriormente mencionado, a finalidade apresentada pelas empresas para fundamentar a conservação dos currículos nas suas bases de dados

²³⁶ Sendo a primeira referência realizada no Considerando 39, quando refere que os “*(...) dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo*”.

²³⁷ BAIRRÃO, Isabel (2019), “*Os dados dos seus colaboradores respeitam o RGPD?*”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acedido a 07 de janeiro de 2022.

²³⁸ GUERRA, Amadeu (2004), “*A Privacidade no Local de Trabalho: As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados Uma Abordagem ao Código do Trabalho*”, s.e., Coimbra, Almedina, p. 169.

tem por base a previsão de abertura de novas vagas e consequente início de novos processos de recrutamento. No entanto, o titular dos dados só estará habilitado à futura vaga se a mesma for criada e anunciada, no decorrer do período da conservação dos seus dados, caso contrário, e ultrapassado esse prazo, os dados devem ser devidamente eliminados.²³⁹

Noutro sentido, há ainda quem defenda a redução deste período, com vista a evitar a acumulação excessiva de dados nas bases de dados. Assim, Patrícia Andreia Batista e Santos defende a redução de 12 para 6 meses, nas situações de recolha de dados aquando da existência de uma vaga aberta, e de 12 meses para 3 a 6 meses, quando os dados digam respeito a candidaturas espontâneas. Tal limitação teria por base o preceito do Considerando 39, onde é identificada a necessidade de “(...) assegurar que o prazo de conservação dos dados seja limitado ao mínimo”, e ainda a rápida desatualização dos currículos.²⁴⁰

Devemos ressaltar que discordamos da redução dos prazos de conservação dos currículos, tendo por base duas questões fulcrais, sendo essas: a dimensão da empresa e a facilidade com que um CV fica desatualizado.

Em primeiro lugar, e no que diz respeito à dimensão da empresa, devemos ter em atenção ao número de funcionários, uma vez que é um fator que pode fazer toda a diferença. Podemos assim assumir que para empresas com um elevado número de trabalhadores (e, por sua vez, uma maior possibilidade de abertura de vagas), a diminuição dos prazos de conservação trará benefícios no que diz respeito ao controlo dos dados armazenados. Evitar-se-ia a acumulação de dados pessoais, na medida em que não seriam armazenados dados desnecessários e desatualizados. Já para as empresas constituídas por um baixo número de funcionários, existiria uma alteração de paradigma, sendo estas seriamente prejudicadas. Presumindo que a possibilidade de abertura de novas vagas seja diretamente proporcional ao número de funcionários da empresa, a reduzida exposição no mercado de trabalho, bem como a falta de meios para a realização da procura e recrutamento de profissionais competentes para uma vaga específica (recrutamento

²³⁹ BAIRRÃO, Isabel (2019), “Os dados dos seus colaboradores respeitam o RGPD?”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acessado a 07 de janeiro de 2022.

²⁴⁰ SANTOS, Patrícia Andreia Batista (2019), “A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 59. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021.

ativo)²⁴¹, e a consequente a redução do prazo de conservação representaria para muitas destas empresas uma dificuldade ainda maior na procura de candidatos. Podemos destacar que muitas destas empresas nem possuiriam uma base de dados da qual constassem currículos de candidatos.

Em segundo lugar, e mantendo o entendimento da CNPD, anteriormente referido, os currículos manter-se-ão atualizados durante um ano²⁴². A redução do prazo de conservação, seria prejudicial para os candidatos que não atualizem tão frequentemente os seus currículos. Ao mesmo tempo não podemos deixar de lado a possibilidade de o currículo ficar desatualizado antes do término do prazo de conservação²⁴³, seja pela frequência em cursos, formações ou qualquer outra situação de carácter profissional de relevância. Neste sentido, seria desprovida de lógica uma redução tão abrupta do prazo de conservação de currículos.

De uma forma geral, caso seja ponderada a redução geral dos prazos de conservação dos currículos, não deve ser estabelecido um limite máximo desse período igual para todas as empresas. Deve ter-se em vista a equidade, e não só a igualdade, atribuindo diferentes prazos para empresas de diferentes dimensões. Por outro lado, seja qual for a alteração proposta ao prazo de conservação de currículos, será sempre necessário, nos termos do artigo 25.º do RGPD, “(...) *ter em conta a proteção de dados desde a conceção e por defeito*”.²⁴⁴

Por último, e não menos importantes, são as situações em que, desde o momento em que consentiu o tratamento dos seus dados, e respetivo armazenamento, até ao momento em que foi contactado pela abertura de nova vaga, o candidato já tenha

²⁴¹ Ver páginas 57 a 61 desta Dissertação.

²⁴² ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 54.

²⁴³ Patrícia Andreia Batista e Santos utiliza ainda como exemplo de dados pessoais que podem resultar na desatualização do CV, a alteração da residência do candidato. Devemos ter em conta que a morada é um dado que não deve constar do conteúdo do currículo (para além de desnecessário pode apresentar riscos para o candidato), devendo o candidato apenas colocar a cidade onde mora, evitando dados mais específicos da sua morada (como por exemplo o código postal, o número de porta, entre outros). Assim, apenas nas situações em que a mudança de residência resulte na mudança de cidade é que será necessário proceder à atualização do CV (através do exercício do direito de retificação, que se encontra disposto no art. 16.º do RGPD). Ver SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 59. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021.

²⁴⁴ *Idem*, p. 59.

conseguido emprego noutra empresa. Neste caso, é-lhe reservado o direito ao apagamento dos seus dados nos termos da alínea a) do n.º 1 do artigo 17.º do RGPD.

4.4 Monitorização dos Trabalhadores Dentro e Fora do Local de Trabalho

A evolução tecnológica é ainda responsável pelo aparecimento de novas formas de controlo dos trabalhadores, com vista ao melhor desempenho das empresas e dos seus funcionários, bem como da proteção do seu património. No entanto, estas operações de tratamento de dados podem representar uma ameaça constante contra a privacidade dos seus trabalhadores, principalmente porque esta monitorização já não se cinge apenas às instalações da entidade empregadora (existindo um controlo dos trabalhadores dentro e fora do local de trabalho). Neste sentido, caso não sejam impostos limites à realização de operações de tratamento no contexto laboral, ou a realização dessas operações não seja transparente, “(...) *existe um risco elevado de que o interesse legítimo dos empregadores na melhoria da eficiência e da proteção do património de uma empresa se transforme numa monitorização intrusiva e injustificável*”.²⁴⁵ O fundamento utilizado pela entidade empregadora para a realização das operações de tratamento resultantes do controlo dos seus trabalhadores deve assim, tal como verificado anteriormente, corresponder a pelo menos uma das situações previstas nas alíneas b), c) e f) do n.º 1 do artigo 6.º do RGPD.

Ressalve-se ainda os dados pessoais tratados através de sistemas de monitorização, não devem ser utilizados para finalidades distintas daquelas para as quais foram recolhidos e tratados. Podemos utilizar como exemplo “(...) *a utilização de sistemas legitimamente instalados para proteger o património para assim monitorizar a disponibilidade, o desempenho e a simpatia dos empregados para com os clientes*”, bem como a “(...) *utilização de dados recolhidos através de câmaras de televisão em circuito fechado para monitorizar regularmente o comportamento e o desempenho dos empregados (...)*”.²⁴⁶

Por outro lado, temos a introdução de uma figura, relativamente recente, que graças à situação pandémica ganhou um novo destaque e, em muitas áreas, veio para ficar.

²⁴⁵ Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017, p. 11.

²⁴⁶ Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017, p. 12.

Referimo-nos ao teletrabalho, que por sua vez levou a uma adaptação dos sistemas de monitorização dos trabalhadores para acompanhar esta alteração de paradigma, sem descurar os interesses legítimos das empresas. Este cenário, da realização das funções laborais em casa, apresentou, sem dúvidas, uma dificuldade maior no que toca a separar a vida privada do trabalhador, da sua vida profissional. No entanto, o próprio desempenho de funções laborais no âmbito do regime de teletrabalho levou há existência de desigualdades entre os trabalhadores da mesma empresa, dado que para alguns o teletrabalho manifestou-se na utilização de dispositivos pessoais no contexto laboral, já para outros, na utilização de dispositivos disponibilizados pela empresa.²⁴⁷

Em todas estas situações é necessário proceder a uma avaliação de impacto da proteção de dados (AIPD)²⁴⁸, uma vez que de todas elas resultam riscos para a privacidade dos trabalhadores (artigo 35.º, n.º 1 do RGPD).

Concluindo, é necessário ter em atenção às especificidades das diversas situações em que há lugar a operações de tratamento de dados (através da utilização de novas tecnologias), das quais podem resultar riscos para os titulares dos mesmos. Referimo-nos, mais concretamente: ao tratamento de dados biométricos, dados de saúde, à utilização de sistemas de geolocalização, bem como de videovigilância, e ao tratamento de dados efetuado no decurso do regime de teletrabalho.

4.4.1 Sistemas Biométricos

Os dados biométricos são todos aqueles que resultam “(...) *de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular (...)*” (artigo 4.º, n.º 14 do RGPD). Neste sentido, devemos considerar como dados biométricos as impressões digitais, a geometria do rosto, a voz, a altura, entre outros.²⁴⁹

Apesar da proibição imposta ao tratamento de dados constantes das categorias especiais de dados²⁵⁰, prevista no artigo 9.º, n.º 1 do RGPD, o seu tratamento é lícito se

²⁴⁷ Ver páginas 77 a 80 desta Dissertação.

²⁴⁸ Ver páginas 40 a 41 desta Dissertação.

²⁴⁹ Atente-se que a utilização destes dados tem vindo, cada vez mais, a ser parte integrante do nosso quotidiano, mesmo que em pequenas porções, como por exemplo para desbloquear um *smartphone*.

²⁵⁰ Ver páginas 13 a 14 desta Dissertação.

Implementação do RGPD no Setor Empresarial

for necessário para o cumprimento de obrigações e exercício de direitos específicos (artigo 9.º, n.º 2, alínea b) do RGPD) e para a execução de um contrato (artigo 6.º, n.º 1, alínea b), ambos do RGPD)²⁵¹.²⁵² O ordenamento jurídico português, mais especificamente a Lei 58/2019, de 8 de agosto, não se prenuncia contrariamente aos dispostos do RGPD, acrescentado apenas, no conteúdo do n.º 6 do seu artigo 28.º, que o tratamento destes dados só é legítimo se for, apenas e somente, utilizado “(...) *para controlo de assiduidade e para controlo de acessos às instalações do empregador (...)*”. No que diz respeito ao contexto laboral, o tratamento de dados biométricos deve ainda respeitar as normas constantes do artigo 18.º do CT²⁵³.

Assim, a utilização de sistemas biométricos é cada vez mais frequente, tendo vindo a ganhar destaque relativamente aos meios anteriormente utilizados. Estes sistemas têm como finalidade apoiar o responsável pelo tratamento na prossecução do cumprimento da obrigação imposta no artigo 202.º do CT. Podemos ainda aditar que, estes sistemas garantem um nível de segurança sem precedentes, uma vez que não registam uma amostra de um dado biométrico, mas sim uma representação digital desse, também denominada de *template*.²⁵⁴ Caso contrário, o funcionamento do sistema em si viola o disposto na parte final do n.º 6 do artigo 28.º da Lei 58/2019, de 8 de agosto, onde se pode ler que tratamento de dados biométricos deve assegurar “(...) *que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados*”.

No entanto, antes da implementação destes sistemas, o responsável pelo tratamento tem de realizar uma avaliação de impacto sobre a proteção de dados (efetuada por si ou pela empresa que criou o sistema), uma vez que estamos na presença de operações de tratamento de dados pessoais através da utilização de novas tecnologias,

²⁵¹ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 66. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acedido a 02 de março de 2021

²⁵² Tal como havíamos tratado nas páginas 54 a 57 desta Dissertação, o consentimento (alínea a), do n.º 1 do art. 6.º do RGPD) não representa um fundamento de licitude de tratamento de dados no contexto laboral, estando por isso excluído da situação em apreço.

²⁵³ Com a exceção do n.º 1 do referido artigo, uma vez que com a entrada em vigor do RGPD deixou de ser necessário notificar a CNPD.

²⁵⁴ Ver descrição detalhada da composição e funcionamento dos sistemas biométricos em GUERRA, Amadeu (2004), “*A Privacidade no Local de Trabalho: As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados Uma Abordagem ao Código do Trabalho*”, s.e., Coimbra, Almedina, pp. 191-193.

suscetível de implicar riscos para os direitos e liberdades dos titulares dos dados (artigo 35.º, n.º 1 do RGPD).²⁵⁵ A avaliação, independentemente de quem a conduza, deve ter em conta: a natureza do tratamento, o seu âmbito, o contexto e as suas finalidades (artigo 35.º, n.º 1 do RGPD). Atente-se ainda que, nos termos das alíneas a) a d) do n.º 7 do artigo 35.º do RGPD, o procedimento de avaliação deve incluir: uma avaliação das operações previstas e da sua finalidade; uma avaliação da necessidade e proporcionalidade dessas operações; uma avaliação de riscos para os direitos e liberdades dos titulares de dados; bem como as medidas previstas para fazer face a esses mesmos riscos.

Efetuada a avaliação, resultando da mesma parecer positivo para a utilização destes sistemas, deve o responsável pelo tratamento comunicar aos seus trabalhadores a pretensão de utilizar esses mesmos sistemas. De forma a garantir aos titulares dos dados o gozo dos seus direitos, deve ainda enunciar qual a finalidade dessas operações. Significa isto, mesmo que o consentimento dos titulares não seja considerado fundamento de licitude destas operações, não deixa por isso de existir a necessidade de manter os titulares de dados informados, nos termos do artigo 13.º, n.º 1 do RGPD. Fica apenas afastada a possibilidade de os titulares dos dados exercerem o direito ao apagamento.²⁵⁶

Por último, resulta do n.º 3 do artigo 18.º do CT, que “*os dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento a que se destinam (...)*”. Apenas devem ser destruídos aquando da cessação do contrato de trabalho que vincula o responsável pelo tratamento ao titular dos dados.

4.4.2 Controlos Médicos

No âmbito da relação contratual é obrigatória, para os trabalhadores, a realização de exames médicos com vista à prevenção de doenças e outros riscos resultantes da sua atividade profissional. Por outras palavras podemos acrescentar que a medicina no

²⁵⁵ Se a entidade já possuir autorização da CNPD para a realização de operações de tratamento de dados biométricos, não necessitam de realizar uma avaliação de impacto sobre a proteção de dados, a não ser que “(...) tenha havido alteração às condições autorizadas para o funcionamento do sistema (...)”, cfr. <https://www.cnpd.pt/organizacoes/areas-tematicas/biometria/>, acessado a 21 de janeiro de 2022.

²⁵⁶ FERREIRA, Carolina Sofia Mendes (2019), “*A Monitorização do Trabalhador e o RGPD*” (Dissertação de Mestrado), Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Leiria, p. 42. Disponível em https://iconline.ipleiria.pt/bitstream/10400.8/4368/1/Disserta%C3%A7%C3%A3o_Carolina-Ferreira.pdf , acessado a 10 de abril de 2021.

Implementação do RGPD no Setor Empresarial

trabalho “(...) *é uma parte integrante e essencial do exercício da atividade profissional*”.²⁵⁷

Neste sentido, e tal como os dados biométricos, os dados relativos à saúde são considerados dados sensíveis, sendo, regra geral, o seu tratamento proibido, nos termos do artigo 9.º, n.º 1 do RGPD. Excetuam-se assim as situações das quais resulte a necessidade de proceder ao tratamento desses dados para efeitos de medicina do trabalho, com vista à avaliação da capacidade de trabalho dos empregados (artigo 9.º, n.º 2, alínea h) do RGPD). O tratamento destes dados deve ser efetuado por um profissional qualificado²⁵⁸, “(...) *obrigado a sigilo profissional ou outra pessoal sujeita a dever de confidencialidade (...)*” (n.º 2 do artigo 29.º da Lei 58/2019 e artigo 9.º, n.º 3 do RGPD, em simultâneo), devendo a entidade empregadora elaborar um contrato, escrito, que vincule as duas partes²⁵⁹.

O tratamento de dados realizado no âmbito da medicina no trabalho deve ser limitado à finalidade a que se destina (artigo 5.º, n.º 1, alínea c) do RGPD), recaindo sobre o responsável pelo tratamento essa mesma responsabilidade (artigo 5.º, n.º 2 do RGPD). Neste seguimento, apenas podem ser objeto de tratamento os dados relativos à identificação do titular, dados de saúde resultantes de exames prévios (realizados no âmbito da medicina do trabalho ou não), dados relativos à sua atividade profissional, dados sobre o risco de doenças profissionais e dados relativos aos hábitos dos titulares (somente se estes estiverem de alguma forma relacionados com a algum conjunto de dados anteriormente fornecidos ou com alguma patologia). Neste contexto, para além dos anteriormente descritos, mais nenhum dado pessoal deve ser objeto de tratamento.²⁶⁰ O responsável pelo tratamento deve ainda ter em conta que, uma vez que estas operações de tratamento se apresentam, “(...) *desde logo, como um risco de discriminação dos trabalhadores*”²⁶¹, este está proibido de elaborar listas consideradas discriminatórias,

²⁵⁷ EKONOMISTA (2022), “*Medicina no Trabalho: tudo o que deve saber*”. Disponível em <https://www.e-konomista.pt/medicina-do-trabalho/>, acessado a 22 de janeiro de 2022.

²⁵⁸ Nos termos do artigo 103.º da Lei n.º 102/2009, de 10 de setembro.

²⁵⁹ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 28.

²⁶⁰ Comissão Nacional de Proteção de Dados (s.d.), “*Deliberação n.º 840/2010*”, pp. 3-4. Disponível em https://www.cnpd.pt/media/pwig2aqa/medicina-trabalho-del_840_2010_.pdf, acessada a 22 de janeiro de 2022.

²⁶¹ *Ibidem*, p. 5.

como por exemplo, “(...) listas de asmáticos, diabéticos, psoriáticos, ou qualquer outra patologia que afete a imunidade do indivíduo”.²⁶²

Relativamente às informações resultantes dos exames realizados neste âmbito, estas estão fora do alcance da entidade empregadora, ou seja, “a informação de saúde deverá ser de acesso restrito ao médico do trabalho (...)”.²⁶³ Às entidades empregadoras apenas é comunicado, através de “ficha de aptidão” devidamente preenchida, se o trabalhador está: apto para desempenhar as funções para as quais foi contratado; apto condicionalmente; inapto condicionalmente; ou inapto definitivamente.²⁶⁴

Outra questão que deve ser tida em conta é a frequência com que devem ser realizados estes controlos. Neste sentido, a realização de exames médicos, no contexto da medicina no trabalho, deve ocorrer de forma periódica. Anualmente para funcionários com idades compreendidas na faixa etária entre os 51 e os 70 anos. Já para os trabalhadores com idades entre os 18 e os 50, os exames devem ser realizados de dois em dois anos.²⁶⁵

Importa ainda ter em atenção as operações de tratamento realizadas no âmbito da pandemia, que atualmente ainda se encontra ativa. Referimo-nos principalmente aos testes rápidos de antigénio (realizados regularmente no âmbito de rastreios obrigatórios no seio das empresas)²⁶⁶, bem como à recolha de dados de saúde, como a temperatura corporal - ambos com objetivo preventivo. O tratamento efetuado deve cumprir todas as disposições legais anteriormente analisadas, diferenciando-se apenas nas situações em que exista um trabalhador infetado com o vírus SARS-Cov-2. Neste caso, o responsável pelo tratamento deve informar os restantes trabalhadores da existência de um caso

²⁶² ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 28.

²⁶³ Comissão Nacional de Proteção de Dados (s.d.), “*Deliberação n.º 840/2010*”, p. 7. Disponível em https://www.cnpd.pt/media/pwig2aqa/medicina-trabalho-del_840_2010_.pdf, acedida a 22 de janeiro de 2022.

²⁶⁴ EKONOMISTA (2022), “*Medicina no Trabalho: tudo o que deve saber*”. Disponível em <https://www.e-konomista.pt/medicina-do-trabalho/>, acedido a 22 de janeiro de 2022.

²⁶⁵ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 27.

²⁶⁶ Orientação n.º 006/2020, de 26 de fevereiro, atualizada a 29 de abril de 2021, da Direção-Geral da Saúde. Disponível em <https://medicisforma.pt/wp-content/uploads/2021/05/Orientacao-no-006.2020-de-26.02.2020-atualizada-a-29.04.2021.pdf>, acedido a 22 de janeiro de 2022.

positivo na empresa, mantendo para si as informações do titular dos dados (inclusive a sua identificação).²⁶⁷

Por último, no que diz respeito aos dados resultantes vigilância da saúde de cada trabalhador, bem como a respetiva ficha médica individual (artigo 46.º, n.º 1, alínea c) e n.º 2 da Lei n.º 102/2009, de 10 de setembro), a entidade empregadora deve, nos termos do artigo 98.º, n.º 5 da Lei n.º 102/2009, de 10 de setembro, mantê-los durante 5 anos. Excetuando-se apenas os registos “(...) *relativos a trabalhadores em situação suscetível de implicar risco para o património genético (nos termos do disposto no artigo 41.º da Lei n.º 102/2009, de 10 de Setembro) (...)*”, do qual resulta a necessidade de conservação durante um período de, pelo menos, 40 anos após o término da exposição (artigo 46.º, n.º 3 da Lei n.º 102/2009, de 10 de setembro).²⁶⁸

4.4.3 Sistemas de Geolocalização

Atualmente são diversos os meios tecnológicos que permitem às entidades empregadoras um maior controlo da produtividade e o cumprimento das obrigações inerentes à relação laboral. Um exemplo destes meios, são os sistemas de geolocalização, que permitem localizar, em tempo real, um objeto e/ou uma pessoa, através de tecnologia GPS (sistema de posicionamento global)²⁶⁹.

No contexto laboral, estes sistemas são maioritariamente utilizados nos veículos da empresa e em dispositivos móveis²⁷⁰, atribuídos aos trabalhadores para prossecução da sua atividade profissional.²⁷¹ A utilização destes sistemas, na medida em que destes resulta a localização exata dos seus trabalhadores, consubstancia, nos termos do n.º 1 do artigo 4.º do RGPD, num tratamento de dados pessoais.²⁷² No entanto, e apesar de não constar do n.º 1 do artigo 9.º do RGPD, os dados de geolocalização são considerados dados sensíveis, visto que representam um elevado risco para os direitos dos seus

²⁶⁷ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 27.

²⁶⁸ Comissão Nacional de Proteção de Dados (s.d.), “*Deliberação n.º 840/2010*”, pp. 8-9. Disponível em https://www.cnpd.pt/media/pwig2aqa/medicina-trabalho-del_840_2010_.pdf, acedida a 22 de janeiro de 2022.

²⁶⁹ O GPS é uma tecnologia em constante evolução e que tem, nos últimos anos, sofrido diversas alterações, positivas, permitindo, nos dias que correm, a localização quase exata de uma pessoa, independentemente do local onde esta se encontre.

²⁷⁰ Dispositivos como telemóveis, computadores, *tablets*, entre outros.

²⁷¹ Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁷² N.º 37 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD, com as devidas alterações para a aplicação ao RGPD.

titulares.²⁷³ Torna-se então imprescindível uma utilização prudente destes sistemas (sejam eles GPS, GSM²⁷⁴ ou Wi-Fi) uma vez que a sua utilização excessiva pode violar os direitos fundamentais dos trabalhadores, tendo em conta que a quantidade de dados resultantes desse tratamento²⁷⁵ permite ao responsável pelo tratamento a elaboração de perfis comportamentais.²⁷⁶

Uma vez que o consentimento do trabalhador não é fundamento de licitude válido para a realização de operações de tratamentos de dados no contexto laboral²⁷⁷, o tratamento de dados de geolocalização apenas é lícito se for necessário para o cumprimento de uma obrigação legal a que o responsável esteja sujeito (alínea c) do n.º 1 do artigo 6.º do RGPD. Poderíamos então questionar qual a obrigação legal inerente a estas operações, uma vez que o CT não apresenta na sua constituição nenhuma referência à geolocalização.²⁷⁸ Neste sentido, a CNPD entendeu que os dispositivos de geolocalização (sejam eles GPS, GSM ou Wi-Fi) constituem, nos termos do artigo 20.º do CT, um meio de vigilância à distância. Através da aplicação das normas do artigo 20.º do CT, resulta do n.º 1 do referido artigo que a utilização destes meios não pode ter como finalidade o controlo do desempenho profissional.²⁷⁹

No que diz respeito aos veículos da empresa²⁸⁰, é lícita a utilização de sistemas de geolocalização sempre que esta tenha como finalidade a proteção e segurança de pessoas e bens “(...) ou quando particulares exigências inerentes à natureza da atividade o

²⁷³ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, pp. 34-35.

²⁷⁴ Sistema Global para Comunicações Móveis, também conhecido por “*Global System for Mobile Communications*” (GSM) é uma tecnologia móvel para telemóveis. Disponível em <https://pt.wikipedia.org/wiki/GSM>, acessido a 22 de janeiro de 2022.

²⁷⁵ Dados relativos aos percursos efetuados, aos locais frequentados, bem como o histórico de movimentos e de tempos de permanência. Cfr. ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 35.

²⁷⁶ N.º 5 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁷⁷ Ver páginas 54-57 desta Dissertação.

²⁷⁸ N.º 48 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁷⁹ Para além do controlo de desempenho do trabalhador, a utilização destes sistemas também “(...) não pode ser utilizada para: (...) b) Fins de prova de cumprimento do contrato (comprovativo de hora, dia e local de entrega de mercadoria, por exemplo); c) Controlo de cumprimento da legislação rodoviária; ou d) Utilização de viatura para fins privados”. Cfr. ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 37.

²⁸⁰ Para um melhor entendimento do funcionamento, ver diagrama de um sistema de monitorização e localização de veículos apresentado em SILVA, Fernando (2016), “*Fórum de Proteção de Dados - Foco: Geolocalização*”, “*Sistemas de Geolocalização e Monitorização de Veículos: Do Início do GPS às Novas Tendências*”, Julho de 2016 (N.º 3), p. 39. Disponível em <https://www.cnpd.pt/comunicacao-publica/revista-forum/>, acessido a 23 de maio de 2020.

justifiquem” (artigo 20.º, n.º 2 do CT). Por outras palavras, podemos afirmar que a instalação destes sistemas nos veículos da empresa é lícita se tiver como finalidade:

- a gestão da frota em serviço externo (apenas nas atividades de assistência técnica externa ou ao domicílio, distribuição de bens, transporte de passageiros, transporte de mercadorias e segurança privada);
- a proteção de bens (apenas nas situações de transporte de materiais perigoso ou materiais de elevado valor²⁸¹).²⁸²

Lurdes Dias Alves acrescenta ainda a possibilidade de instalar sistemas de geolocalização nos veículos da empresa, limitando o acesso do responsável pelo tratamento de dados. Ou seja, só seria possível aceder aos dados de localização do veículo em caso de furto de uma das viaturas. Para além desta, o responsável pelo tratamento deve, não só garantir que os trabalhadores têm conhecimento da existência de um sistema de geolocalização nos veículos que lhes são atribuídos, como também implementar mecanismos que permitam aos seus colaboradores limitar o funcionamento destes sistemas, desconectando-os, fora do seu horário de trabalho. Neste seguimento, a CNPD acrescenta ainda “(...) *que não pode haver monitorização da geolocalização da viatura quando esta estiver a ser utilizada pelo trabalhador para fins privados*”.²⁸³ Deste modo, estes mecanismos teriam como objetivo a minimização dos dados nos termos da alínea c) do n.º 1 do artigo 5.º do RGPD.²⁸⁴

Por sua vez, no que diz respeito aos dispositivos móveis inteligentes, a CNPD considera excessivo e desproporcional o tratamento de dados de geolocalização com vista à proteção de bens.²⁸⁵ Esta desproporcionalidade parte do princípio de que estes dispositivos (principalmente os telemóveis), na sua grande maioria das vezes acompanham o trabalhador, ao qual foram atribuídos, para todo o lado. Tal situação não acontece com os veículos. Assim, e uma vez que consideramos o tratamento realizado pelos sistemas de geolocalização instalados nos veículos da empresa, suscetível de violar

²⁸¹ Devemos considerar transporte de valor muito elevado quando esse seja superior a 10.000,00€ (dez mil euros).

²⁸² ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 36.

²⁸³ N.º 140 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁸⁴ *Ibidem*, pp. 34-36

²⁸⁵ N.º 74 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

a privacidade dos trabalhadores ao ponto da sua utilização ser tão limitada, os dados de localização obtidos pelas operações de tratamento realizadas nestes dispositivos móveis seriam ainda mais detalhados e específicos, logo mais intrusivos. Mesmo nas situações em que o responsável justifique a instalação destes sistemas nos dispositivos móveis com a necessidade de proteger esses bens, o tratamento não é considerado lícito nos termos do n.º 2 do artigo 20.º do CT, visto que este já tem ao seu alcance ferramentas como um MDM (*Mobile Device Management*)²⁸⁶ que, no caso de furto, lhe permitem apagar remotamente toda a informação.²⁸⁷

Relativamente aos períodos de conservação, os dados resultantes do tratamento realizado com vista à gestão de frota em serviço externo, devem ser conservados por um período máximo de uma semana, sendo posteriormente “(...) sujeitos a um processo de anonimização para posterior análise estatística (...)”.²⁸⁸ O referido prazo de conservação aplica-se também aos dados resultantes do tratamento realizado com vista à proteção de bens²⁸⁹, bem como aos dados recolhidos de dispositivos de geolocalização, quando instalados para fins exclusivos de participação criminal em caso de furto²⁹⁰.

4.4.4 Sistemas de Videovigilância

Por sistemas de videovigilância devemos entender que são todos os sistemas eletrónicos, de vigilância à distância, que procedam à captação e recolha de imagem, suscetíveis de captar informações relativas a uma ou mais pessoas, identificando-as (n.º 1 do artigo 4.º do RGPD). Neste sentido, “(...) *não é necessário que integrem imagens explícitas de pessoas, mas tão só imagens que permitam identificar ou localizar pessoas*”.²⁹¹ A utilização destes sistemas tem vindo a suscitar diversos problemas, principalmente no que diz respeito à possível violação do direito à imagem (artigo 79.º do CC) e à reserva da vida privada do titular dos dados.

²⁸⁶ É um sistema de tem como objetivo a gestão de dispositivos móveis, bem como a sua proteção, monitorização, podendo ser utilizado por operadoras de telecomunicações e empresas. Retirado de https://pt.wikipedia.org/wiki/Gerenciamento_de_dispositivos_m%C3%B3veis, acessido a 23 de janeiro de 2022.

²⁸⁷ N.º 81 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁸⁸ N.º 98 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁸⁹ N.º 100 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁹⁰ N.º 103 da Deliberação n.º 7680/2014, 28 de outubro de 2014, da CNPD.

²⁹¹ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 38.

Implementação do RGPD no Setor Empresarial

No que diz respeito à utilização de sistemas de videovigilância no contexto laboral²⁹², tal como se verifica relativamente à utilização de qualquer outro meio de vigilância à distância, a mesma é proibida se tiver como finalidade o controlo do desempenho dos trabalhadores²⁹³ (artigo 20.º, n.º 1 do CT). Será lícita a sua utilização apenas se tiver “(...) *por finalidade a proteção e segurança de pessoas e bens ou particulares exigências inerentes à natureza da atividade o justifiquem*” (artigo 20.º, n.º 2 do CT). Exemplo desta limitação é o Acórdão do Supremo Tribunal de Justiça, de 18 de maio de 2005²⁹⁴, que atribui ao empregador a possibilidade da utilização destes sistemas sempre que tenha por finalidade a proteção e a segurança de pessoas e bens, sendo que “(...) *essa utilização deverá traduzir-se numa forma de vigilância genérica, destinada a detetar factos, situações ou acontecimentos incidentais, e não numa vigilância diretamente dirigida aos postos de trabalho ou ao campo de ação dos trabalhadores*”. Cabe então à entidade empregadora a instalação de um circuito interno de televisão, também conhecido por *closed-circuit television* (CCTV), não podendo as câmaras incidir sobre: as vias públicas e propriedades limítrofes; os locais de digitação de códigos de caixas multibanco ou terminais de ATM; o interior de áreas reservadas a clientes ou utentes (como por exemplo, lavabos, salas de espera, provadores de vestuário, entre outras); e o interior de áreas reservadas aos trabalhadores (como por exemplo refeitórios, vestiários, lavabos, entre outras).²⁹⁵ Para além destes requisitos, interessam ainda ter em atenção o tipo de equipamento (câmaras fixas ou móveis), o ângulo de filmagem, a possibilidade de ampliar ou aproximar a imagem, bem como funções de bloqueio de imagem.²⁹⁶ É ainda de ressaltar que apesar de lícita a utilização destes

²⁹² Ver Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de junho de 2017, p. 24.

²⁹³ Neste sentido, a captação de imagens realizada através de sistemas de videovigilância utilizados para finalidades que não a proteção e segurança de pessoas e bens, não constitui meio de prova em processo relacionado com o desempenho profissional do trabalhador. Por outras palavras, “*a consequência legal dessa utilização ilícita dos meios de vigilância à distância é a invalidade da prova obtida para efeitos disciplinares*”. Cfr. Acórdão do Tribunal da Relação do Porto, Processo n.º 231/14.6TTVNG.P1, de 17 de dezembro de 2014. Consultado a 22 de janeiro de 2022, retirado de <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d8b30e6de8712dd580257dc700551703?OpenDocument>.

²⁹⁴ Acórdão do Supremo Tribunal de Justiça, Processo n.º 05S3139, de 18 de maio de 2005. Consultado a 22 de janeiro de 2022, retirado de <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument>.

²⁹⁵ Alíneas a) a d) do n.º 2 do art. 19.º da Lei 58/2019, de 8 de agosto.

²⁹⁶ Ver Grupo de Trabalho do Artigo 29.º - “*Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância*”, adotado em 11 de fevereiro de 2004, p. 20 e GUERRA, Amadeu (2004), “A

sistemas, é proibida a captação de som durante a permanência de clientes e trabalhadores nas instalações da empresa (n.º 4 do artigo 19.º da Lei 58/2019).

Existem ainda instituições e empresas que devido às exigências inerentes à natureza da sua atividade (artigo 20.º, n.º 2 do CT) justifica a utilização de sistemas de videovigilância. Como por exemplo, “(...) *Banco de Portugal; Banca; Instituições de Crédito e Sociedades Financeiras; Estabelecimentos de restauração e bebidas que disponham de salas destinadas a dança, Armeiros; Sucateiros, entre outras atividades*”.²⁹⁷

Independente da finalidade para a qual sejam utilizados os sistemas de videovigilância, à entidade empregadora é atribuída a obrigação de informar todos os trabalhadores da existência desses, a sua localização, bem como as finalidades é que se destinam. Para além da comunicação deve ainda “(...) *afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo*” (artigo 20.º, n.º 3 do CT).²⁹⁸

No que respeita ao acesso às imagens captadas, o mesmo não é permitido, exceto quando necessário no âmbito de um processo penal, mesmo que para o apuramento de responsabilidade disciplinar (n.º 4 e 5 do artigo 28.º da Lei 58/2019). Deste modo, cabe a todas as pessoas que tenham acesso a essas gravações o dever de guardar sigilo, sendo ainda proibida a cessão ou cópia dessas (n.º 3 e 3 do artigo 31.º da Lei 34/2013).

Finalmente, no que respeita ao período de conservação das imagens captadas, as mesmas devem ser preservadas, “(...) *em registo codificado, pelo prazo de 30 dias contados desde a respetiva captação (...)*”, tendo o responsável pelo tratamento de dados a obrigação de as eliminar no prazo máximo de 48 horas (n.º 2 do artigo 31.º da Lei 34/2013). No entanto, o prazo anteriormente referido é apenas o limite máximo, perante o qual deve a entidade empregadora conservar esses dados. Caso esta considere

Privacidade no Local de Trabalho: As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados Uma Abordagem ao Código do Trabalho”, s.e., Coimbra, Almedina, pp. 356-357.

²⁹⁷ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 43.

²⁹⁸ Complementar com as alíneas do n.º 5 do artigo 31.º da Lei 34/2013, de 16 de maio

necessário, nos termos do artigo 21.º, n.º 3 do CT, a aplicação de um prazo mais reduzido, na prossecução da finalidade a que se destina a utilização destes sistemas, deve fazê-lo.²⁹⁹

4.4.5 Teletrabalho

Não menos importante, no que toca à proteção de dados no contexto laboral, é o regime em que a prestação da atividade laboral é realizada fora das instalações físicas da empresa³⁰⁰, também conhecido por teletrabalho³⁰¹. Esta é uma figura que tem vindo a ganhar cada vez mais destaque, principalmente a partir do momento em que o Governo português considerou este regime obrigatório (para as prestações de trabalho compatíveis com este)³⁰² como medida de combate à propagação do vírus SARS-Cov-2³⁰³ (como por exemplo, no artigo 6.º do Decreto n.º 2-A/2020, de 20 de março).

Neste sentido, e de uma forma mais detalhada, devemos compreender por teletrabalho, toda e qualquer “(...) *prestação laboral realizada com subordinação jurídica, habitualmente fora da empresa e através do recurso a tecnologias de informação e de comunicação*” (artigo 165.º do CT). Resultam assim, da definição de teletrabalho dois pontos que merecem ser analisado individualmente. Referimo-nos à subordinação jurídica e à utilização de tecnologias de informação e de comunicação.

No que respeita à subordinação jurídica, devemos ter em atenção que independentemente de se tratar de um empregado que já desempenha as suas funções naquela empresa, ou de um trabalhador admitido para realização das suas funções através do regime de teletrabalho, é imprescindível a existência de um contrato (artigo 166.º, n.º 1 do CT). No entanto, o mesmo deve revestir forma escrita, tendo em vista, se necessário, comprovar a estipulação do regime de teletrabalho (artigo 166.º, n.º 7 do CT).

²⁹⁹ FERREIRA, Carolina Sofia Mendes (2019), “*A Monitorização do Trabalhador e o RGPD*” (Dissertação de Mestrado), Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Leiria, p. 54. Disponível em https://iconline.ipleiria.pt/bitstream/10400.8/4368/1/Disserta%C3%A7%C3%A3o_Carolina-Ferreira.pdf, acedido a 10 de abril de 2021.

³⁰⁰ FALCÃO, David & TOMÁS, Sérgio Tenreiro (2016), “*Lições de Direito de Trabalho: A Relação Individual de Trabalho*”, 4.ª Edição, Coimbra, Almedina, p. 136.

³⁰¹ É uma figura relativamente recente no ordenamento jurídico português, uma vez que foi pela primeira vez regulamentado pela Lei n.º 99/2003, de 27 de agosto, também conhecida por Código de Trabalho de 2003, cfr. SOUSA, Duarte Abrunhosa (2016), “*O Enquadramento Legal do Teletrabalho em Portugal*”, “*Derecho Social y Empresa*”, p. 3. Disponível em <https://www.ajj.pt/publicacoes/3>, acedido a 10 de janeiro de 2022.

³⁰² REBELO, Glória (2021), “*O Teletrabalho na Era Digital: Estudos Laborais*”, s.e., Coimbra, Almedina, pp. 27-30.

³⁰³ O Governo português já por diversas vezes, recorreu ao regime de teletrabalho, com carácter obrigatório, como medida de combate à pandemia, tendo última vez sido já no ano de 2022.

Implementação do RGPD no Setor Empresarial

Por sua vez, os recursos dos quais carece o trabalhador para a sua prestação laboral devem ser garantidos pela entidade empregadora, que para além destes deve assegurar a respetiva instalação, manutenção e o pagamento de despesas inerentes à sua utilização (artigo 168.º do CT).

No entanto, a execução das suas tarefas fora das instalações físicas da empresa, não garante à entidade empregadora maior poder ou controlo sobre o trabalhador abrangido por este regime, muito menos a capacidade de o discriminar (artigo 23.º do CT). Nesta perspetiva, o CT reconhece, no seu artigo 169.º, a igualdade de direitos e deveres para todos os trabalhadores, “(...) nomeadamente no que se refere a formação e promoção ou carreiras profissionais, limites do período normal de trabalho e outras condições de trabalho, segurança e saúde no trabalho e reparação de danos emergentes de acidente de trabalho ou doença profissional”, independente do local onde estes desempenhem as suas funções. Esta igualdade aplica-se também ao direito à reserva da intimidade da vida privada (artigo 16.º do CT), devendo a entidade empregadora respeitar a privacidade destes, bem como os tempos de descanso (artigo 170.º CT).

Assim, relativamente ao controlo à distância dos trabalhadores em regime de teletrabalho, é necessário ter em atenção às orientações da CNPD.³⁰⁴ Numa primeira fase devemos debruçarmo-nos sobre a presunção do artigo 168.º do CT, uma vez que a obrigatoriedade do regime de teletrabalho imposta pelos sucessivos estados de emergência não permitiu às entidades empregadores fornecer meios tecnológicos suficientes a todos os seus colaboradores. Muitos destes acabaram por fazer uso dos seus dispositivos privados para a satisfação das necessidades da empresa, garantindo que o exercício das suas funções seria desempenhado tal como se se encontrasse nas instalações da mesma. Neste contexto, devemos ter em conta “(...) que independentemente da propriedade dos instrumentos de trabalho, no regime de teletrabalho o empregador mantém os poderes de direção e de controlo da execução da prestação laboral”³⁰⁵.³⁰⁶

³⁰⁴ Orientações da CNPD sobre o controlo à distância em regime de teletrabalho, de 17 de abril de 2022. Disponível em <https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/trabalho/>, acedido a 21 de janeiro de 2022.

³⁰⁵ Exemplo disso mesmo é o disposto no n.º 2 do art. 170.º do CT, onde se encontra prevista a possibilidade de visita à residência do trabalhador, efetuada entre as 09:00h e as 19:00h, com o objetivo de controlar a atividade laboral.

³⁰⁶ Orientações da CNPD sobre o controlo à distância em regime de teletrabalho, de 17 de abril de 2022, pp. 1-2. Disponível em <https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/trabalho/>, acedido a 21 de janeiro de 2022.

Implementação do RGPD no Setor Empresarial

Contudo, tal como se verifica na situação dos dados de geolocalização³⁰⁷, o ordenamento jurídico português carece de normas específicas relativamente à proteção de dados no regime de teletrabalho. Até lá devemos aplicar as normas constantes do artigo 20.º do CT (de epígrafe “*meios de vigilância à distância*”), nomeadamente no que diz respeito à proibição da utilização de meios de vigilância à distância com vista ao controlo do desempenho dos trabalhadores (artigo 20.º, n.º 1 do CT).³⁰⁸ Contudo, do disposto no n.º 2 do referido artigo, resulta a possibilidade de utilização de dispositivos ou *softwares*, por parte da entidade empregadora, que tenham como objetivo a proteção e segurança de pessoas e bens.

Sabemos ainda que, não obstante da limitação imposta no artigo 168.º, n.º 3 do CT, relativa à não utilização dos instrumentos de trabalho, para fins que não as funções laborais, há sempre trabalhadores que não cumprem este limite. O não cumprimento deste disposto resulta no aumento do “(...) *risco de acesso não autorizado aumenta e pode resultar na perda ou destruição das informações, incluindo os dados pessoais dos empregados ou clientes*”.³⁰⁹ A fim de limitar essas possibilidades poderiam então as entidades empregadoras considerar a utilização de *softwares* (quer nas instalações da empresa, quer na computação na nuvem³¹⁰) que “(...), *para além do rastreamento do tempo de trabalho e de inatividade, registam as páginas de Internet visitadas, a localização do terminal em tempo real, as utilizações dos dispositivos periféricos (ratos e teclados), fazem captura de imagem do ambiente de trabalho, observam e registam quando se inicia o acesso a uma aplicação, controlam o documento em que se está a trabalhar e registam o respetivo tempo gasto em cada tarefa (...)*”. Consequentemente, a CNPD considera desproporcional e abusiva a utilização desses *softwares*, justificando que estes “(...) *recolhem manifestamente em excesso dados pessoais dos trabalhadores, promovendo o controlo do trabalho num grau muito mais detalhado do que aquele que pode ser legitimamente realizado no contexto da sua prestação nas instalações da*

³⁰⁷ Ver páginas 71 a 74 desta Dissertação.

³⁰⁸ ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina, p. 48.

³⁰⁹ Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de junho de 2017, p. 20.

³¹⁰ Ver Grupo de Trabalho do Artigo 29.º - “*Parecer 05/2012 relativo a computação em nuvem*”, adotado em 1 de julho de 2017.

entidade empregadora”.³¹¹ Por outras palavras, a CNPD atenta assim que a utilização destes viola a disposição do artigo 169.º, n.º 1 do CT.

No entanto, a CNPD considera a existência de uma exceção ao acima preceituado, o controlo e registo de tempos de trabalho de funcionários que se encontrem a desempenhar as suas funções em regime de teletrabalho. Cabe então à entidade empregadora a implementação de um *software* que tenha como objetivo o registo dos períodos da atividade laboral, tal como se das instalações da empresa se tratasse. Caso contrário, se o software escolhido pela entidade não limitar o seu tratamento apenas aos dados estritamente necessários, o mesmo não poderá ser utilizado, dado que viola o princípio da proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD).³¹²

Em suma, é da responsabilidade da entidade empregadora a avaliação do risco que o regime do teletrabalho representa para a sua empresa, principalmente no que diz respeito a possíveis perdas ou até destruição de informações da mesma. Deve assim aplicar “(...) *as medidas adequadas para assegurar um nível de segurança adequado* (...)”³¹³, garantindo que a monitorização dos trabalhadores em regime de teletrabalho só tem como objeto o trabalho realizado por este, e não a sua vida privada.³¹⁴

³¹¹ Orientações da CNPD sobre o controlo à distância em regime de teletrabalho, de 17 de abril de 2022, p. 2. Disponível em <https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/trabalho/>, acessado a 21 de janeiro de 2022.

³¹² *Idem*, p. 3.

³¹³ Art. 32.º, n.º 1 do RGPD.

³¹⁴ SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa, p. 69. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessado a 02 de março de 2021.

CONCLUSÃO

Podemos concluir, com a realização deste trabalho, que o RGPD veio criar um paradigma mais justo, coeso e uniforme, no que diz respeito à atribuição de um maior controlo dos titulares, sobre os seus dados e sobre as operações de tratamento aos quais estão sujeitos.

No que respeita à aplicação das normas existentes, relativas ao tratamento de dados pessoais realizado no contexto laboral, é-nos possível compreender as dificuldades que esta representa para o setor empresarial. Para além das diferentes especificidades de cada operação de tratamento, existe ainda alguma dificuldade no acesso a todas as normas aplicáveis a estas operações, uma vez que as mesmas se encontram dispersas (especialmente no que respeita aos Pareceres e Orientações da CNPD). Somando a essas dificuldades a inexistência de normativos específicos para algumas das operações realizadas neste âmbito, estamos na presença de maiores adversidades no que respeita à aplicação do RGPD. Referimo-nos, mais concretamente, às operações às quais é necessária a aplicação das normas constantes dos artigos 20.º e 21.º do CT, relativas à utilização de meios de vigilância à distância, que, para além de que se encontram parcialmente desatualizadas, não representam, na sua totalidade, as particularidades de cada operação. Ressalva-se ainda que, a atualização dessas normas, principalmente no que concerne à exigência de autorização da Comissão Nacional da Proteção de Dados para a utilização de meios de vigilância à distância (artigo 21.º, n.º 1 e 2 do RGPD), é considerada uma necessidade, desde a entrada em vigor do RGPD.

Outra temática, que mereceu o devido destaque ao longo desta dissertação, está relacionada com os fundamentos de licitude das operações de tratamento de dados realizadas neste contexto. Em especial, quais as diferenças que apresenta o consentimento dos trabalhadores, como fundamento de licitude das operações de tratamento realizadas ainda antes da existência de um vínculo laboral (durante os processos de recrutamento), das operações realizadas no âmbito das relações laborais.

Podemos considerar que existe ainda um longo caminho a percorrer até que seja possível verificar-se um total respeito pela proteção de dados pessoais e um consequente *compliance*, de uma forma geral, com as normas estatuídas no RGPD. Prova disso mesmo é que só no mês de dezembro de 2021, se verificou a aplicação de coimas no valor de

Implementação do RGPD no Setor Empresarial

10.719.550,00€ (dez milhões, setecentos e dezanove mil e quinhentos e cinquenta euros), relativas ao incumprimento das normas constantes do RGPD.³¹⁵ No entanto, consideramos que esta exposição representa um ponto de vista diferente perante a necessidade da aplicação das regras estatuídas neste Regulamento.

Por fim, gostaríamos de sugerir, para além das atualizações anteriormente referidas, possíveis tópicos com relevância mais que suficiente para serem base de escrutínio de trabalhos de investigação futuros. Referimo-nos mais concretamente ao consentimento do titular dos dados como fundamento de licitude e as suas limitações, bem como qualquer uma das operações de tratamento enunciadas ao longo desta dissertação, dado que, devido às suas especificidades e particularidades, beneficiariam de uma análise individual e aprofundada, de forma a conceder-lhes a visibilidade que realmente merecem.

³¹⁵ MyDataPrivacy (s.d.), “*Coimas RGPD em dezembro 2021!*”. Disponível em <https://mydataprivacy.eu/coimas-rgpd-em-dezembro-de-2021-2/>, acessado a 01 de fevereiro de 2022.

BIBLIOGRAFIA

- ALVES, Lurdes Dias (2020), “*Proteção de Dados Pessoais no Contexto Laboral: O Direito à Privacidade do Trabalhador*”, s.e., Coimbra, Almedina. ISBN 9789724085814
- CALVÃO, Filipa Urbano (s.d.), “*Direito da Proteção de Dados Pessoais: Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*”, s.e., Universidade Católica Editora, Porto. ISBN 9789898835406
- CANOTILHO, J. J. Gomes & MOREIRA, Vital (2007), “*Constituição da República Portuguesa Anotada: Volume I*”, 4.^a Edição Revista, Coimbra, Almedina.
- CORDEIRO, A. Barreto Menezes (2020), “*Direito da Proteção de Dados: À luz do RGPD e da Lei n.º 58/2019*”, Reimpressão, Coimbra, Almedina. ISBN 9789724083049
- FALCÃO, David & TOMÁS, Sérgio Tenreiro (2016), “*Lições de Direito de Trabalho: A Relação Individual de Trabalho*”, 4.^a Edição, Coimbra, Almedina. ISBN 9789724064727
- FAZENDEIRO, Ana (2020), “*Nova Lei de Proteção de Dados Pessoais*”, s.e., Coimbra, Almedina. ISBN 9789724084176
- GOMES, Mário M. Vargês (2006), “*O Código da Privacidade e da Proteção de Dados Pessoais na Lei e na Jurisprudência*”, s.e., Edições Centro Atlântico, Vila Nova de Famalicão. ISBN 9896150222
- GUERRA, Amadeu (2004), “*A Privacidade no Local de Trabalho: As Novas Tecnologias e o Controlo dos Trabalhadores através de Sistemas Automatizados Uma Abordagem ao Código do Trabalho*”, s.e., Coimbra, Almedina. ISBN 9724022242
- LEITÃO, Luís Menezes (2019), “*Direito do Trabalho*”, 6.^a Edição, Coimbra, Edições Almedina. ISBN 9789724080901
- PAIS DE VASCONCELOS, Pedro (2019), “*Teoria Geral do Direito Civil*”, 9.^a Edição, Coimbra, Edições Almedina. ISBN 9789724081847
- REBELO, Glória (2021), “*O Teletrabalho na Era Digital: Estudos Laborais*”, s.e., Coimbra, Almedina. ISBN 9789724092607
- SALDANHA, Nuno (2018), “*Novo Regulamento Geral de Proteção de Dados: O que é? A quem se aplica? Como implementar?*”, s.e., Lisboa, FCA - Editora de Informática. ISBN 97897228898

Implementação do RGPD no Setor Empresarial

- SALDANHA, Nuno (s.d.), “*RPDG Guia para uma Auditoria de Conformidade: Dados, Privacidade, Implementação, Controlo, Compliance*”, s.e., Lisboa, FCA - Editora de Informática. ISBN 9789727229055

FONTES E PUBLICAÇÕES ELETRÓNICAS

- Agência dos Direitos Fundamentais da União Europeia, Conselho da Europa (2014), “*Manual da Legislação Europeia sobre a Proteção de Dados*”, Luxemburgo, Serviço de Publicações da União Europeia. Disponível em <https://op.europa.eu/pt/publication-detail/-/publication/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1>, acessido a 01 de fevereiro de 2022.

- BAIRRÃO, Isabel (2019), “*Os dados dos seus colaboradores respeitam o RGPD?*”. Disponível em <https://rhmagazine.pt/os-dados-dos-seus-colaboradores-respeitam-rgpd/>, acessido a 07 de janeiro de 2022.

- BRANCO, Flávia Machado Castelo (2018), “*O Regulamento Geral sobre a Proteção de Dados: Direitos dos Utilizadores*” (Dissertação de Mestrado), Instituto Superior de Contabilidade e Administração de Coimbra, Coimbra. Disponível em <https://comum.rcaap.pt/handle/10400.26/27829>, acessido a 04 de março de 2021.

- Comissão Nacional de Proteção de Dados (s.d.), “*Áreas temáticas: Videovigilância*”. Disponível em <https://www.cnpd.pt/organizacoes/areas-tematicas/videovigilancia/>, acessido a 22 de janeiro de 2022.

- Comissão Nacional de Proteção de Dados (s.d.), “*Direito ao apagamento dos dados*”. Disponível em <https://www.cnpd.pt/cidadaos/direitos/direito-ao-apagamento-dos-dados/>, acessido a 23 de junho de 2021.

- Comissão Nacional de Proteção de Dados (s.d.), “*Deliberação n.º 7680/ 2014, 28 de outubro de 2014*”. Disponível em https://www.cnpd.pt/media/zvxmdfad/del_7680-2014_geo_laboral.pdf, acessida a 22 de janeiro de 2022.

- Comissão Nacional de Proteção de Dados (s.d.), “*Deliberação n.º 840/2010*”. Disponível em https://www.cnpd.pt/media/pwig2aqa/medicina-trabalho-del_840_2010_.pdf, acessida a 22 de janeiro de 2022.

- Comissão Nacional de Proteção de Dados (s.d.), “*O que somos e quem somos*”. Disponível em <https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/>, acessido a 07 de junho de 2021.

Implementação do RGPD no Setor Empresarial

- Comissão Nacional de Proteção de Dados (s.d.), “*Orientações e Recomendações: Trabalho*”. Disponível em <https://www.cnpd.pt/organizacoes/orientacoes-e-recomendacoes/trabalho/>, acessido a 15 de outubro de 2021.
- DE HERT, PAUL & LAMMERAN, Hans (2013), “*Protection of Personal Data in Work-Related Relations*”. Disponível em [https://www.europarl.europa.eu/thinktank/pt/document/IPOL-LIBE_ET\(2013\)474440](https://www.europarl.europa.eu/thinktank/pt/document/IPOL-LIBE_ET(2013)474440), acessido a 29 de janeiro de 2022.
- Diário da República Eletrónico (s.d.), “*Princípio da integridade e confidencialidade*”. Disponível em <https://dre.pt/dre/LinkLexionarioAntigo?termoId=143859891>, acessido a 29 de abril de 2021.
- Diário da República Eletrónico (s.d.), “*Princípio da lealdade (tratamento de dados pessoais)*”. Disponível em <https://dre.pt/dre/lexionario/termo/principio-lealdade-tratamento-dados-pessoais>, acessido a 27 de janeiro de 2022.
- Diário da República Eletrónico (s.d.), “*Princípio da responsabilidade (tratamento de dados pessoais)*”. Disponível em <https://dre.pt/dre/lexionario/termo/principio-responsabilidade-tratamento-dados-pessoais>, acessido a 18 de janeiro de 2022.
- EKONOMISTA (2022), “*Medicina no Trabalho: tudo o que deve saber*”. Disponível em <https://www.e-konomista.pt/medicina-do-trabalho/>, acessido a 22 de janeiro de 2022.
- FERREIRA, Carolina Sofia Mendes (2019), “*A Monitorização do Trabalhador e o RGPD*” (Dissertação de Mestrado), Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Leiria. Disponível em https://iconline.ipleiria.pt/bitstream/10400.8/4368/1/Disserta%C3%A7%C3%A3o_Carolina-Ferreira.pdf, acessido a 10 de abril de 2021.
- FIDALGO, Vitor Palmela (2019), “*O Direito à Portabilidade de Dados Pessoais*”, Revista de Direito e Tecnologia, Volume 1, NO. 1. Retirado de <https://blook.pt/publications/publication/cec4178f8a58/>, acessido a 26 de junho de 2021.
- HENRIQUES, Sérgio Coimbra, & LUÍS, João Vares (2019), “*Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral*”, “*Anuário de Proteção de Dados*”. Disponível em http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf, acessido a 29 de janeiro de 2022.

Implementação do RGPD no Setor Empresarial

- Lei n.º 58/2019, de 8 de agosto. Disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3118&tabela=leis&nverso=&so_miolo=, acessido a 05 de abril de 2021.
- MyDataPrivacy (s.d.), “*Coimas RGPD em dezembro 2021!*”. Disponível em <https://mydataprivacy.eu/coimas-rgpd-em-dezembro-de-2021-2/>, acessido a 01 de fevereiro de 2022.
- NASCIMENTO, Ricardo & GAMA, Alexandre (2019), “*RGPD em Contexto Laboral*”, “*Boletim da Ordem dos Advogados*”, N.º 24 Setembro 2019. Disponível em <https://portal.oa.pt/publicacoes/boletim/edicoes-de-2019/edicoes-pdf-para-download/>, acessido a 10 de agosto de 2021.
- OPENLIMITS (2017), “*RGPD - GLOSSÁRIO: TODOS OS TERMOS QUE PRECISA DE CONHECER*”. Disponível em <https://www.openlimits.pt/pt/thinking-ahead-blog/glossario-rgpd-regulamento-europeu-protacao-dados/?all=1>, acessido a 12 de maio de 2022.
- Orientação n.º 006/2020, de 26 de fevereiro, atualizada a 29 de abril de 2021, da Direção-Geral da Saúde (DGS). Disponível em <https://medicisforma.pt/wp-content/uploads/2021/05/Orientacao-no-006.2020-de-26.02.2020-atualizada-a-29.04.2021.pdf>, acessido a 22 de janeiro de 2022.
- SANTOS, Carlos Manuel Carvalho dos (2015), “*Proteção de Dados dos Trabalhadores*” (Dissertação de Mestrado), Lisboa, Universidade Autónoma de Lisboa. Disponível em <https://repositorio.ual.pt/bitstream/11144/1856/1/Prote%c3%a7ao%20de%20Dados%20dos%20Trabalhadores.pdf>, acessido a 15 de abril de 2021.
- SANTOS, Patrícia Andreia Batista (2019), “*A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral*” (Dissertação de Mestrado), Universidade Nova de Lisboa, Lisboa. Disponível em https://run.unl.pt/bitstream/10362/89834/1/BatistaSantos_2019.pdf, acessido a 02 de março de 2021.
- SILVA, Fernando (2016), “*Fórum de Proteção de Dados - Foco: Geolocalização*”, “*Sistemas de Geolocalização e Monitorização de Veículos: Do Início do GPS às Novas Tendências*”, Julho de 2016 (N.º 3). Disponível em <https://www.cnpd.pt/comunicacao-publica/revista-forum/>, acessido a 23 de maio de 2020.

Implementação do RGPD no Setor Empresarial

- SOUSA, Duarte Abrunhosa (2016), “*O Enquadramento Legal do Teletrabalho em Portugal*”, “*Derecho Social y Empresa*”. Disponível em <https://www.ajj.pt/publicacoes/3>, acessado a 10 de janeiro de 2022.
- Universidade de Coimbra (s.d.), “*Informação Administrativa e Proteção de Dados*”; “*Anonimização e Pseudonimização*”. Disponível em https://www.uc.pt/ptecao-de-dados/ptecao_dados_pessoais/anonimizacao, acessado a 07 de setembro de 2021.
- UTTER (s.d.), “*A IMPLEMENTAÇÃO DESTE TIPO DE MEDIDAS PELAS ORGANIZAÇÕES, QUANDO POSSÍVEL, ADEQUADO E PROPORCIONAL, PODERÁ MANIFESTAR-SE COMO UMA EVIDÊNCIA DE CUMPRIMENTO DO REGULAMENTO*”. Disponível em <https://utter.pt/anonizacao-e-pseudonizacao-saiba-o-que-e/>, acessado a 27 de janeiro de 2022.
- Your Europe (2021), “*A Proteção de Dados ao abrigo do RGPD*”. Disponível em https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm#shortcut-7, acessado a 14 de maio de 2021.

JURISPRUDÊNCIA

- Acórdão do Supremo Tribunal de Justiça, Processo n.º 05S3139, de 18 de maio de 2005. Consultado a 22 de janeiro de 2022, retirado de <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument>.
- Acórdão do Tribunal da Relação do Porto, Processo n.º 231/14.6TTVNG.P1, de 17 de dezembro de 2014. Consultado a 22 de janeiro de 2022, retirado de <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d8b30e6de8712dd580257dc700551703?OpenDocument>.
- Acórdão do Tribunal de Justiça (Grande Secção), Processo C-507/17, de 24 de setembro de 2019. Consultado a 22 de junho de 2021, retirado de https://curia.europa.eu/juris/document/document_print.jsf?docid=218105&text=&dir=&doclang=PT&part=1&occ=first&mode=DOC&pageIndex=0&cid=4245208#Footnote*.
- Procuradoria-Geral Distrital de Lisboa (s.d.), “*Sumários do STJ (Boletim) - Laboral*”, “*ACSTJ de 08-02-2006*”. Disponível em https://www.pgdlisboa.pt/jurel/stj_mostra_doc.php?nid=22142&codarea=3, acessado a 17 de janeiro de 2022.

UNIÃO EUROPEIA

- Comissão Europeia (s.d.), “*A proteção de dados ao abrigo do RGPD*”, “*O que se entende por dados pessoais?*”. Disponível em https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm, acessado a 07 de janeiro de 2022.
- Comissão Europeia (s.d.), “*O meu empregador pode obrigar-me a dar consentimento para utilizar os meus dados?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_pt, acessado a 07 de janeiro de 2022.
- Comissão Europeia (s.d.), “*O que são autoridades de proteção de dados (APD)?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_pt, acessado a 07 de junho de 2021.
- Comissão Europeia (s.d.), “*O que são dados pessoais?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt, acessado a 07 de janeiro de 2022.
- Comissão Europeia (s.d.), “*O que significa a proteção de dados «desde a conceção» e «por defeito»?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt, acessado a 29 de junho de 2021.
- Comissão Europeia (s.d.), “*Posso ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis?*”. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_pt, acessado a 30 de maio de 2021.
- Comissão Europeia (s.d.), “*Regulamentos, diretivas e outros atos legislativos*”. Disponível em https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt, acessado a 26 de maio de 2021.
- Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046>, acessado a 03 de março de 2021.

Implementação do RGPD no Setor Empresarial

- Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*”, revistas e adotadas pela última vez em 4 de outubro de 2017.
- Grupo de Trabalho do Artigo 29.º - “*Orientações relativas à transparência na aceção do Regulamento 2016/679*”, adotadas em 29 de novembro de 2017.
- Grupo de Trabalho do Artigo 29.º - “*Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*”, adotadas em 28 de novembro de 2017, última redação revista e adotada em 10 de abril de 2018.
- Grupo de Trabalho do Artigo 29.º - “*Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*”, adotadas em 3 de outubro de 2017, com a última redação revista e adotada em 6 de fevereiro de 2018.
- Grupo de Trabalho do Artigo 29.º - “*Orientações sobre o direito à portabilidade dos dados*”, adotadas em 13 de dezembro de 2016, com a última redação revista e adotada em 5 de abril de 2017.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 1/2010 sobre os conceitos de «responsável pelo tratamento» e «subcontratante»*”, adotado em 16 de fevereiro de 2010.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 2/2017 sobre o tratamento de dados no local de trabalho*”, adotado em 8 de Junho de 2017.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 3/2010 sobre o princípio da responsabilidade*”, adotado em 13 de Julho de 2010.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 3/2013 sobre a limitação da finalidade*”, adotado em 2 de abril de 2013.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância*”, adotado em 11 de fevereiro de 2004.
- Grupo de Trabalho do Artigo 29.º - “*Parecer 4/2007 sobre o conceito de dados pessoais*”, adotado em 20 de junho de 2007.

Implementação do RGPD no Setor Empresarial

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>, acedido a 19 de fevereiro de 2021.
- Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da proteção de dados pessoais na União Europeia ([2011/2025\(INI\)](#)). Disponível em https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323_PT.html, acedido a 03 de março de 2021.
- Tratado de Lisboa, que entrou em vigor a 1 de dezembro de 2009. Disponível em https://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf, acedido 26 de janeiro de 2022.