NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

RGPD aplicado nas PME portuguesas

Gustavo de Carvalho Silva

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

RGPD APLICADO NAS PME PORTUGUESAS

por

Gustavo de Carvalho silva

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Gestão de Informação, Especialização em Gestão do Conhecimento e Inteligência de Negócio

Orientador: Mauro Castelli

fevereiro 2019

AGRADECIMENTOS

A minha esposa Vanessa e a minha filha Vitória por terem abdicado de alguns momentos de família e por me manterem motivado nas fases mais difíceis.

Um agradecimento especial ao meu orientador, o Professor Mauro Castelli, pelo seu apoio e disponibilidade.

Também quero agradecer aos meus pais, a minha irmã Elizabete, o meu cunhado António e o meu sobrinho Diogo por toda a ajuda que me deram.

RESUMO

O Regulamento Geral sobre a Proteção de Dados (RGPD) regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, com entrada em aplicação a 25 de maio de 2018.

Vem introduzir não só novas regras como também elevadas coimas em caso de incumprimento, o que exige uma atenção cuidada das organizações que lidam e possuem à sua guarda dados pessoais.

As PME, dado as suas características dimensionais, poderão encontrar muitas dificuldades na implementação do novo regulamento. É preciso compreender como as PME lidam com dados pessoais e de que forma se adaptaram para cumprir o regulamento durante este primeiro ano de implementação

Para esta dissertação, foi conduzido um inquérito às PME portuguesas com o objetivo de avaliar que tipo de dados estas tratam, o conhecimento que têm do regulamento e como se adaptaram as novas regras.

PALAVRAS-CHAVE

RGPD; PME; CNPD; SME; dados pessoais; tratamento

ABSTRACT

The General Data Protection Regulation (RGPD) regulates the protection of individuals regarding the processing of personal data and the free movement of such data, which entered into force on 25 May 2018.

It introduces not only new rules but also high fines in case of non-compliance, which requires the careful attention of the organizations that handle and keep individual's personal data.

SMEs, given their dimensional characteristics, may encounter many difficulties in implementing the new regulation. We need to understand how SMEs handle personal data and how they have adapted to comply with the regulation during this first year of implementation.

For this dissertation, a survey was conducted on Portuguese SMEs to assess what type of data they deal with, their knowledge of the regulation and how the new rules have been adapted.

KEYWORDS

GDPR; PME; CNPD; SME; personal data

ÍNDICE

1. Introdução 1
2. RGPD 3
   2.1. Enquadramento histórico 3
   2.2. Legislação 4
      2.2.1. Objeto e objetivos 4
      2.2.2. Definições 5
      2.2.3. Princípios 7
      2.2.4. Direitos 10
   2.3. RGPD e as PME 11
   2.4. Autoridade de controlo 13
      2.4.1. CNPD 14
3. PME 16
   3.1. PME em Portugal 16
   3.2. Desafio Digital 17
4. Descrição do estudo realizado 19
   4.1. Metodologia 19
   4.2. Caracterização das PME da amostra 19
   4.3. Conhecimento do RGPD 21
   4.4. Tipo de dados pessoais e aquisição 22
   4.5. Finalidades e Licitude 25
   4.6. Adaptação 27
   4.7. Direitos de acesso e esquecimento 29
5. Conclusões 32
6. Limitações e Recomendações para Trabalhos Futuros 34
7. Bibliografia 35
8. Anexos 37

ÍNDICE DE FIGURAS

Figura 2.1 – Percentagem de agregados familiares com acesso à Internet na União Europeia 3
Figura 3.1 – Total de PME em Portugal 16
Figura 3.2 – Total de PME por região em Portugal 17
Figura 3.3 – Empresas com presença na internet por dimensão 18
Figura 4.1 – Distribuição das PME por dimensão 19
Figura 4.2 – Distribuição das PME por antiguidade 19
Figura 4.3 – Distribuição das PME por região 20
Figura 4.4 – Distribuição das PME por setor de atividade 20
Figura 4.5 – Função do inquirido na PME 20
Figura 4.6 – Aquisição do conhecimento do RGPD 21
Figura 4.7 – Aquisição do conhecimento do RGPD por dimensão 21
Figura 4.8 – Nível de conhecimento do RGPD 22
Figura 4.9 – Categoria de dados alvo de tratamento 23
Figura 4.10 – Quantidade de categorias de dados pessoais 23
Figura 4.11 – Categorias de dados pessoais únicas 23
Figura 4.12 – Setores com tratamento de 1 categoria de dados pessoais 24
Figura 4.13 – Formas de aquisição dos dados pessoais 24
Figura 4.14 – registo de tratamento modelo CNPD resumido 25
Figura 4.15 – Finalidades para o tratamento de dados 25
Figura 4.16 – Fundamentos de Licitude para o tratamento de dados 26
Figura 4.17 – Marketing e Vendas com consentimento 26
Figura 4.18 – Prova de tratamento lícito 27
Figura 4.19 – Auditoria aos dados pessoais 27
Figura 4.20 – Dificuldades em implementar o RGPD 27
Figura 4.21 – Ações tomadas para implementar o RGPD 28
Figura 4.22 – Ações tomadas sobre dados antes do RGPD 29
Figura 4.23 – Receio de multa por incumprimento do RGDP 29
Figura 4.24 – Facilidade de acesso aos dados 30
Figura 4.25 – Tempo que demora a prestar a informação da utilização dos dados pessoais . 30
Figura 4.26 – Facilidade de pedido de esquecimento 31
Figura 4.27 – Tempo que demora a apagar os dados pessoais 31

ÍNDICE DE TABELAS

Tabela 2.1 - Características do consentimento 8
Tabela 2.2 - Legislação nacional valores das coimas 14
Tabela 4.1 - Tabela categorias de dados pessoais 22
Tabela 4.2 - Tabela ações tomadas 28

LISTA DE SIGLAS E ABREVIATURAS

B2B	Business to business
B2C	Business to consumer
CEPD	Comité Europeu para a Proteção de Dados
CNPD	Comissão Nacional de Proteção de Dados
EPD	Encarregado da Proteção de Dados
EU	União Europeia
PIB	Produto Interno Bruto
PME	Pequenas e médias empresas
RGPD	Regulamento Geral sobre a Proteção de Dados
SI	Sistemas de informação
SME	Small and medium-sized enterprises

1. **INTRODUÇÃO**

A 25 de Maio de 2018 entrou em vigor o Regulamento (EU) 2016/679 do Parlamento Europeu e o Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados, mais conhecido como RGPD (Regulamento Geral sobre a Proteção de Dados).

Este regulamento faz uma revisão à definição de dados pessoais, define novas regras para o tratamento dos dados pessoais, direitos dos titulares dos dados, obrigações para as organizações que tratam os dados e medidas de contraordenação para o incumprimento.

Cada estado membro pode definir, em matérias específicas, legislações próprias que complementem o regulamento, mas não o podem sobrepor. Em Portugal, até Julho de 2019, não existia legislação para a execução do RGPD. Sendo assim, a lei de Proteção de Dados 67/98 continuou em vigor em tudo que não contrariasse o RGPD.

Para as empresas, este regulamento obriga profundas alterações na forma como habitualmente trabalham com os dados pessoais que possuem, nomeadamente no que diz respeito a procedimentos internos, recolha dos dados pessoais e das ferramentas utilizadas no processamento destes dados.

No contexto das micro, pequenas e médias empresas (PME), este desafio torna-se maior dado as características dimensionais das empresas em termos de recursos tecnológicos, humanos e monetários.

Num relatório publicado em Maio de 2019 pela GDPR.eu (GDPR.eu, 2019) foi realizado um inquérito a 716 PME sediadas em Espanha, Reino Unido, França e Irlanda sobre o cumprimento do RGPD. As conclusões apontam para que cerca de 50% das PME não cumprem 2 fatores críticos do RGPD - licitude e transparência.

Neste mesmo relatório, apesar de algumas PME não acreditarem que os reguladores irão aplicar multas às pequenas empresas, muitas mais citaram que o receio das multas é a principal razão para o cumprimento do regulamento.

Em 2016, as PME representavam 99.9% das empresas portuguesas sendo que destas 96,2% são da categoria de microempresas.[1] Com coimas que podem ir a valores de 20 milhões de Euros ou até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior (consoante o montante que for mais elevado), o incumprimento do regulamento poderá representar a incapacidade de continuar com a atividade.

Um fator para as PME terem sucesso é ter uma estratégia de marketing digital e social. Desta forma, as PME podem expor os seus produtos e serviços a um número mais vasto de clientes potencializando o número de vendas. No que diz respeito aos dados pessoais, esta estratégia potencializa o aumento do tratamento de dados pessoais e muitas das vezes, devido as dimensões

[1] Fonte: PORDATA (Fonte dos dados: INE - Sistema de Contas Integradas das Empresas)

das empresas, esta tarefa é feita por empresas de outsourcing, o que aumenta a necessidade de controlo sobre os dados pessoais.

Este trabalho pretende analisar como as PME portuguesas estão a lidar com esta nova realidade após pouco mais de 1 ano da implementação do regulamento. Para tal, é necessário perceber:

- Qual o nível de conhecimento que as PME têm sobre o Regulamento?
- Sobre que tipo de dados pessoais as PME efetuam o tratamento? Como são obtidos?
- Quais as finalidades e quais consideram que são os argumentos que tornam o tratamento lícito?
- Que ações foram tomadas para implementar o regulamento?
- Estão a ser assegurados os direitos dos titulares dos dados pessoais? Nomeadamente o direito de acesso e o direito a ser esquecido?

De seguida é feita uma análise rigorosa do RGPD, das suas características e principais implicações nas PME. É feita também uma análise das características das PME em Portugal e os seus desafios. Por fim, são descritos os resultados e análises feitas através do inquérito realizado junto de algumas PME portuguesas.

2. RGPD

2.1. ENQUADRAMENTO HISTÓRICO

Em 24 de outubro de 1995, foi publicada a primeira diretiva europeia relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Diretiva 95/46/CE). Esta diretiva esteve em vigor até 25 de maio de 2018, data da entrada do regulamento RGPD.

A diretiva 95/46/CE reconhecia a privacidade como um direito fundamental e definia os padrões mínimos para que os países membros as transpusessem em leis de proteção de dados. Em Portugal, a Lei nº 67/98 (Lei de Proteção de Dados Pessoais) transpôs esta diretiva para a ordem jurídica portuguesa que entrou em vigor à 27 de outubro de 1998, um dia após ter sido publicada em Diário da República.

Dada a característica de diretiva, e de acordo com a legislação europeia, cada país pôde aplicar diferentes níveis de proteção dos direitos das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros. Esta disparidade na execução e aplicação da diretiva 95/46/CE entre membros da União, por vezes constituíam um obstáculo ao exercício das atividades económicas a nível da União, distorcia a concorrência e impedia as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da união.[2]

Para além disso, existia um sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica[2]. Se olharmos para o ano em que a diretiva foi publicada, 1995, a internet tinha uma utilização diferente dos tempos modernos. Para além do número de utilizadores ser menor, a quantidade de dados pessoais fornecidos também era consideravelmente menor.

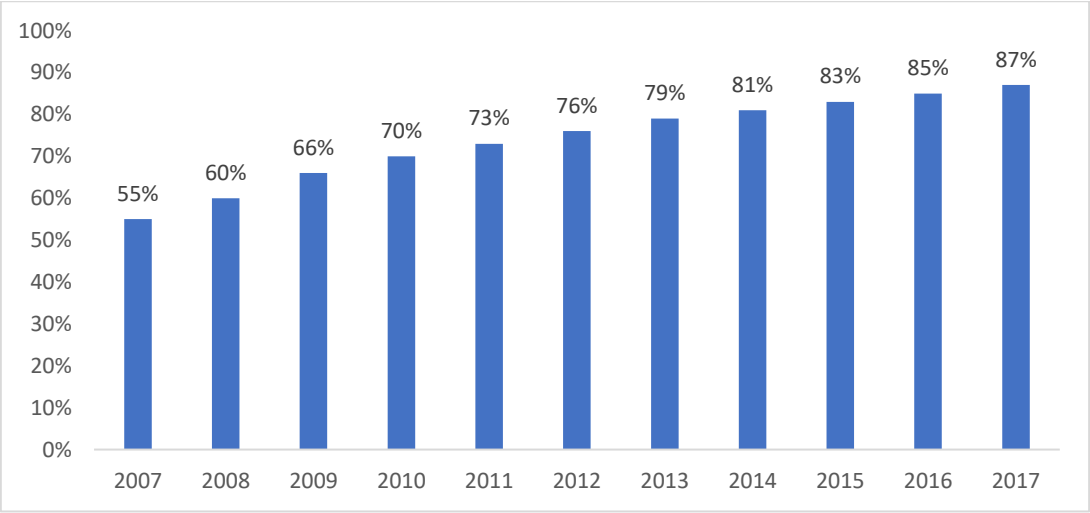

Figura 2.1 – Percentagem de agregados familiares com acesso à Internet na União Europeia[3]

[2] RGPD (9)

[3] Fonte EuroState: https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ci_in_h&lang=en

Todos estes fatores contribuíram para que em janeiro de 2012 fosse proposta a reformulação da diretiva, de forma a fortalecer o direito a proteção de dados online e aumentar a economia digital na Europa. O resultado deste trabalho foi publicado em maio de 2016, através do Regulamento (EU) 2016/679 do Parlamento Europeu e o Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados, mais conhecido por RGPD.

2.2. LEGISLAÇÃO

Segundo a legislação europeia, regulamentos têm caráter geral, são obrigatórios em todos os seus elementos e diretamente aplicáveis em todos os países da União Europeia (UE). Desta forma, é garantida a uniformidade na sua aplicação. Cada Estado-Membro teve que avaliar o impacto deste regulamento face às suas leis anteriores (Jiahong, 2016).

Em pontos explicitamente referenciados no regulamento, os Estados-Membros podem definir legislação própria que complemente o regulamento. A título de exemplo, o Artigo 8º referente às condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação, refere que se a criança tiver menos de 16 anos, o tratamento dos dados só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. No entanto os Estados-Membros podem definir uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.[4]

O documento tem um total de 88 páginas. Inicia com 173 recitais que dão contexto e informação adicional para compreender o RGPD, seguido de 99 artigos que definem as regras para os Estado-Membros implementarem o regulamento.

2.2.1. Objeto e objetivos

O primeiro artigo do regulamento define os seguintes objeto e objetivos:

Estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais

Estes objetivos não diferem do que era definido pela diretiva 95/46/CE, que estabelecia:

Os Estados-membros assegurarão, em conformidade com a presente directiva, a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à protecção assegurada por força do nº 1.

[4] RGPD artigo 8º

Uma alteração mais significativa, é a abrangência territorial do regulamento. Enquanto que a diretiva 95/46/CE tinha com base onde os dados eram fisicamente tratados, no RGPD a abrangência está relacionada com o fato dos dados pessoais serem de titulares residentes no território da União.

O artigo 3º do documento cita:

Para empresas estabelecidas na EU: *aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.*

Para empresas fora da EU: *aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:*

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público

Ou seja, mesmo empresas que não sejam sediadas ou representadas em um país do Estado-Membro, mas que prestem produtos ou serviços a cidadãos europeus devem cumprir com o regulamento. Empresas que processem dados de cidadãos europeus fora da União, também são obrigados a cumprir com o regulamento.

2.2.2. Definições

De forma a ser clara a compreensão das regras, convém olharmos para as definições de dados pessoais e de tratamento de dados. De acordo com o artigo 4º do RGPD, **dados pessoais** (1) são:

informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Uma pessoa singular ser identificável, no contexto das tecnologias principalmente, ganha grande importância. O conceito de identificável, pode ser visto como métodos diretos ou indiretos, para tentar identificar uma pessoa dentro de um grupo de pessoas. Por outras palavras, os dados geralmente não serão pessoais se estes só puderem ser associados a um grupo de pessoas opostamente a uma pessoa singular (Bygrave, 2003).

A simples possibilidade de uma pessoa singular poder ser identificada através de um dado, é o suficiente para considerá-lo como dado pessoal.

Tratamento de dados (2):

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;

Pela definição de tratamento de dados e pelos exemplos contidos no regulamento, é possível concluir que praticamente todas as empresas fazem algum tipo de tratamento de dados. Na gestão dos recursos humanos, por exemplo, é natural que as empresas detenham dados pessoais dos colaboradores, tais como: nome, morada, data de nascimento, habilitações, número da conta bancária, entre outros. As questões que as empresas devem colocar para cada dado pessoal que possuem são:

Com quais finalidades estes dados são usados? Onde estão armazenados? Quem tem acesso a este dados? Por quanto tempo são retidos? No exemplo acima, se um colaborador sair da empresa, existe alguma obrigação legal que permita reter os dados? Mesmo que exista, qual é o tempo máximo de retenção?

Todas estas questões irão conduzir a análise se o tratamento dos dados está a ser feito de uma forma lícita, ou seja, dentro das regras impostas pelo regulamento. Caso não estejam, as empresas devem tomar medidas para assegurar o cumprimento, tais como: apagar os dados, anonimiza-los ou pedir o consentimento aos titulares dos dados. Caso contrário, correm o risco de serem aplicadas coimas de valores elevados.

Existem também categorias especiais de dados pessoais que não podem ser alvo de tratamento:

Artigo 9º(1): *É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*

O artigo 9º(2) do regulamento prevê algumas exceções que licitam o tratamento de dados especiais. Para além do consentimento do titular dos dados (a), destacam-se 2 casos no contexto das PME:

(b) *Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de* ***legislação laboral****, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;*

(h) *Se o tratamento for necessário para efeitos de* ***medicina*** *preventiva ou* ***do trabalho****, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.o 3;*

Sendo que as garantias previstas no artigo 9º (3) implicam que os dados sejam *tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional*.

Outras definições importantes são a dos principais atores no tratamento de dados pessoais (artigo 4º):

Responsável pelo tratamento (7)*, 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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;*

Subcontratante (8)*, uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;*

Destinatário (9)*, uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;*

Terceiro (10)*, a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;*

2.2.3. Princípios

Conforme visto no capítulo Objeto e objetivos, o artigo 1º do RGPD descreve:

O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Estas regras estão presentes no artigo 5º na forma de princípios para o tratamento de dados pessoais.

Princípio da licitude, lealdade e transparência (artigo 5º 1. a)

Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

De acordo com o artigo 6º do RGPD, o tratamento dos dados pessoais é lícito quando se verifica o (a) consentimento, (b) um contrato, (c) obrigações jurídicas, (d) interesses vitais, (e) interesse público ou (f) interesse legitimo.

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O **consentimento** é uma das formas de legitimar o tratamento dos dados e deve ser pedido quando o tratamento não se enquadra em nenhuma das restantes categorias. Sendo que o consentimento deve ser:

Livre	O Consentimento não pode ser condicionado, ou seja, se o cliente não der Consentimento não tem acesso a um determinado produto ou serviço. O Titular dos dados pode recusar ou retirar o Consentimento sem ser prejudicado. O Consentimento deve ser tão fácil de retirar quanto de dar.
Informado	O texto do Consentimento deve ter uma linguagem clara, simples e de fácil acesso. O Titular dos dados deve ser informado sobre as Finalidades a que o Tratamento se destina e sobre o direito de retirar o Consentimento a qualquer momento.
Específico	O Titular dos dados deve poder dar um Consentimento para cada Finalidade do Tratamento (exemplo: dar autorização para marketing é diferente de dar autorização para marketing de empresas terceiras).
Expresso	O Consentimento deverá ser um ato positivo (declaração escrita – inclusive em formato eletrónico – ou declaração oral). O silêncio, as opções pré-validadas ou a omissão não deverão constituir um Consentimento.
Evidenciável	O responsável deve poder demonstrar que o Titular dos dados deu o seu Consentimento para o Tratamento dos seus Dados Pessoais, ou seja, deve ser possível registar e comprovar a data/hora em que o Consentimento foi obtido, o canal de comunicação utilizado e a versão do Consentimento.

Tabela 2.1 - Características do consentimento

O consentimento para o tratamento de dados de crianças, menores de 16 anos, requerer que o mesmo seja dado pelos titulares das responsabilidades parentais da criança. Isto pode levantar questões de como é que pode ser assegurado que o consentimento foi de fato dado pelo responsável parental e não por uma outra pessoa, principalmente em acessos online. O RGPD, no

ponto 2 do artigo, refere apenas que é o responsável pelo tratamento dos dados que deve assegurar todos os esforços para que esta garantia exista.

Limitação das finalidades (artigo 5º 1. b)

Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»);

Os Dados Pessoais são tratados exclusivamente para as finalidades determinantes da sua recolha e apenas serão tratados para finalidades distintas quando legalmente permitido e mediante prestação de informação ao respetivo titular.

Minimização dos dados (artigo 5º 1. c)

Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

Exatidão (artigo 5º 1. d)

Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

Limitação da conservação (artigo 5º 1. e)

Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);

Integridade e confidencialidade (artigo 5º 1. e)

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 acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

Estas regras realçam a condição de que o titular dos dados tem o máximo direito sobre os mesmos e obriga as empresas a manterem registo dos consentimentos e mecanismos para apagar os dados sempre que solicitado pelo titular dos dados. Para além disto, o pedido de consentimento não pode ser dado por omissão, tem que ser um ato explícito. Deve ser claro no propósito, não pode ser agrupado com outros consentimentos nem serem referenciados em politicas de privacidade das empresas.

Perante estes princípios as empresas têm que rever e eventualmente adaptar procedimentos internos, políticas da empresa e sistemas de informação.

As empresas têm que saber exatamente onde os dados estão localizados (exemplos: servidores, Desktops, portáteis, pens, cloud) e para cada um deles saber identificar a(s) finalidade(s) do tratamento. Se alguma das finalidades for com base no consentimento, as empresas têm que ser capazes de provar que o mesmo foi obtido de forma clara, concisa, transparente, inteligível e facilmente acessível a forma e propósito do processamento e do intervalo de tempo em que os seus dados serão armazenados. Para além disso, terão que ser capazes de exercer sobre os dados que possuem os direitos assegurados aos titulares dos dados.

Trata-se de uma tarefa árdua, mesmo para pequenas empresas que possuem poucos dados pessoais, assegurar tal controlo.

2.2.4. Direitos

Os direitos dos titulares dos dados já estavam presentes na diretiva 95/46/CE, o RGPD reforçou estes direitos e introduziu 2 novos. As empresas têm que ser capazes de responder aos direitos dos titulares sempre que estes o desejarem.

Direito de acesso (Artigo 15º)
Direito a obter a confirmação de quais são os seus Dados Pessoais que são tratados e informação sobre os mesmos, como por exemplo, quais as Finalidades do Tratamento, quais os prazos de conservação, entre outros. Direito a ver/ouvir ou obter cópia, por exemplo das faturas, dos acordos escritos ou das chamadas em que é interveniente e que são gravadas.

Direito de retificação (Artigo 16º)
Direito de pedir a retificação dos seus Dados Pessoais que se encontrem inexatos e de completar os Dados Pessoais incompletos, como por exemplo a morada, o NIF, o email, os contactos telefónicos, ou outros.

Direito ao apagamento dos dados ou "direito a ser esquecido" (Artigo 17º)
Direito de obter o apagamento dos seus Dados Pessoais, desde que não se verifiquem fundamentos válidos para a sua conservação, como por exemplo os casos em que a empresa tem de conservar os dados para cumprir uma obrigação legal de preservação para investigação, deteção e repressão de crimes ou porque se encontra em curso um processo judicial.

Direito à portabilidade - Novo (Artigo 20º)
Direito de receber os dados que forneceu em formato digital de uso corrente e de leitura automática ou de solicitar a transmissão direta dos dados para outra entidade que passe a ser o novo responsável pelos seus Dados Pessoais, desde que seja tecnicamente possível.

Direito de oposição (Artigo 21º)
Direito de se opor, a qualquer momento a um tratamento de dados, como por exemplo no caso do tratamento de dados para fins de marketing. O responsável pelo tratamento cessa o tratamento dos

dados pessoais, a não ser que se verifiquem interesses legítimos que prevaleçam sobre os seus interesses, direitos e liberdades, como por exemplo de defesa de um direito num processo judicial.

Direito de limitação - Novo (Artigo 18º)
Direito a solicitar a limitação do tratamento dos Dados Pessoais, sob forma de: (i) suspensão do Tratamento ou (ii) limitação do âmbito do Tratamento a certas categorias de dados ou Finalidades de Tratamento.

Para além de terem que ser capazes de satisfazer os direitos dos titulares dos dados, sempre que for exercido um dos direitos dos artigos 16º (ratificação), 17º (apagamento) ou 18º (limitação), o artigo 19º descreve que o responsável pelo tratamento deve comunicar, a cada destinatário a quem os dados pessoais tenham sido transmitidos, o direito que foi exercido. É feita a salvaguarda se esta comunicação se tornar impossível ou implicar um esforço desproporcionado.

2.3. RGPD E AS PME

O regulamento da proteção de dados é aplicável, no que diz respeito às empresas, a qualquer pessoa singular ou coletiva que exerce uma atividade económica. No entanto, são reconhecidas as características especiais das PME. No recital 13 é dito:

Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades

A conservação do registo de atividades é descrita no artigo 30º (Registos das atividades de tratamento) e dita que cada responsável pelo tratamento e, sendo caso disso, o seu representante deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade. Deve ser capaz de disponibilizar, a pedido, registo à autoridade de controlo.

As PME não são obrigadas a manter este registo, exceto se o tratamento de dados que seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados, ou dados pessoais relativos a condenações penais e infrações.

Outro aspeto relevante para as PME é a de avaliar a necessidade de nomear um Encarregado da Proteção de Dados (EPD). O EPD, conforme citado pelo Comité Europeu para a Proteção de Dados (CEPD), é um pilar da responsabilidade, pode facilitar a conformidade e, além disso, propiciar uma vantagem competitiva às empresas. Servem também de intermediários entre as partes interessadas (Europeia, Orientações sobre os encarregados da proteção de dados (EPD)).

De acordo com o artigo 39º do RGPD, as principais funções do EPD são:

(a) *Informar e aconselhar o responsável pelo tratamento ou o subcontratante e os trabalhadores que tratem os dados, a respeito das suas obrigações e de outras disposições de proteção de dados*
(b) *Controla a conformidade com o regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do*

subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes

(c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização

(d) Coopera com a autoridade de controlo

(e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento

No entanto, as PME só terão que designar um EPD nos seguintes casos, de acordo com o artigo 37º 1.:

*b) As **atividades principais** do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em **grande escala**;*

*c) As **atividades principais** do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em **grande escala** de categorias especiais de dados nos termos do artigo 9.o e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o.*

O RGPD não define o que constitui *atividades principais* e *grande escala*. Estes termos tornam-se vagos e podem conduzir a uma má avaliação da necessidade de designar um EPD. A diretriz sobre o encarregado de proteção dos dados, do Comité Europeu para a Proteção de Dados (CEPD), fornece algumas indicações, mas não existe uma regra fácil e clara.

A diretriz (Europeia, Orientações sobre os encarregados da proteção de dados (EPD)) diz que:

As «**atividades principais**» podem entender-se como as operações essenciais para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, as quais incluem também, todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante.

Alguns exemplos prestados pela diretriz:

1. o tratamento de dados relativos à saúde, designadamente os registos de saúde dos doentes, deve ser considerado uma das atividades principais de qualquer hospital, pelo que os hospitais devem nomear EPD.
2. uma empresa de segurança privada exerce a vigilância de um conjunto de centros comerciais privados e de espaços públicos. A vigilância é a atividade principal da empresa, que, por sua vez, está indissociavelmente ligada ao tratamento de dados pessoais. Por conseguinte, esta empresa deve igualmente designar um EPD.
3. Por outro lado, todas as organizações exercem determinadas atividades de apoio, nomeadamente a remuneração dos seus trabalhadores ou atividades comuns de apoio informático. Trata-se de exemplos de funções de apoio necessárias para a atividade principal ou a área de negócio central da organização. Embora sejam necessárias ou essenciais, por norma estas atividades são consideradas funções acessórias e não a atividade principal.

A mesma diretriz diz quais são os fatores que as empresas devem considerar na avaliação de um tratamento em «larga escala»:

- O número de titulares de dados afetados – como número concreto ou em percentagem da população em causa ;
- O volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento
- A duração, ou permanência, da atividade de tratamento de dados ;
- O âmbito geográfico da atividade de tratamento ;

Alguns exemplos de tratamentos em larga escala citados pela diretriz:

- o tratamento de dados de doentes no exercício normal das atividades de um hospital ;
- o tratamento de dados de viagem das pessoas que utilizam o sistema de transportes públicos de uma cidade (p. ex., através de passes de viagem) ;
- o tratamento em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços ;
- o tratamento de dados de clientes no exercício normal das atividades de uma companhia de seguros ou de um banco ;
- o tratamento de dados pessoais para fins de publicidade comportamental por um motor de busca ;
- o tratamento de dados (conteúdo, tráfego, localização) por operadoras telefónicas ou por fornecedores de serviços de internet ;

Alguns exemplos que não constituem tratamento de grande escala citados pela diretriz:

- o tratamento de dados de pacientes por um médico ;
- o tratamento de dados pessoais relacionados com condenações penais e infrações por um advogado ;

Face ao exposto, caberá a cada empresa avaliar se necessita designar um EPD consonante ao tratamento que façam dos dados pessoais. É expectável que a maioria das PME não necessitem de um EPD, no entanto, é importante que documentem a análise interna efetuada de forma a poderem comprovar o cumprimento das obrigações do responsável pelo tratamento.

2.4. AUTORIDADE DE CONTROLO

De acordo com o artigo 51º, é designada por **autoridade de controlo**, *uma ou mais autoridades públicas independentes, cuja responsabilidade e a de fiscalizar a aplicação do regulamento do RGPD. Só assim, é possível defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União* (1).

Em comparação com a legislação anterior, a autoridade de controlo assume um papel de fiscalizador. Deixaram de ser necessárias as notificações e emissões de autorização para tratamento de dados pessoais. Desta forma, existe uma maior responsibilização sobre as empresas que devem ser capazes de fazer prova do tratamento lícito dos dados pessoais. Terão também que notificar a autoridade de controlo sempre que existir um significativo risco para os direitos dos titulares dos dados pessoais.

De acordo com o artigo 57º, a autoridade de controlo terá um papel de controlar a aplicação do regulamento, sensibilizar os responsáveis do tratamento e subcontratantes para as suas responsabilidades, aconselhar a respeito das medidas legislativas, gerir reclamações, cooperar com outras autoridades de controlo, investigar sobre a aplicação do regulamento, entre outras.

2.4.1. CNPD

Em Portugal, a Comissão Nacional de Proteção de Dados (CNPD) assegura o papel de *autoridade de controlo*, dando assim continuidade ao trabalho que já realizava no seguimento da Diretiva 95/46/CE.

Até 30 de Abril de 2019, cerca de 1 ano após a entrada em vigor do RGPD, a CNPD aplicou 4 coimas ao abrigo do regulamento. Foram aplicadas 3 coimas a entidades privadas e 1 coima a um hospital público, que totalizaram um montante de 424 mil euros (Calvão, 2019).

As empresas privadas não foram reveladas, por esta razão não é possível saber se foram grandes empresas ou PME. No entanto, é revelado que, muitas vezes, estiveram em causa problemas relacionados com a não garantia dos direitos dos cidadãos, dando como exemplo um dos casos em que não foi concedido o direito de acesso à informação.

Essas coimas foram aplicadas numa altura em que a legislação nacional não existia. A proposta de lei nº 120/XIII/3ª, para assegurar a execução do RGPD, na ordem jurídica interna, foi aprovado em Assembleia da República no dia 14 de Junho de 2019, promulgado pelo Presidente da República a 26 de Julho de 2019 e tornou-se na Lei nº 58/2019 em 8 de Agosto de 2019 com a sua publicação em Diário da República. Esta lei tem como objetivo complementar o regulamento em matérias específicas.

Nesta lei, é de destacar o reconhecimento da CNPD como autoridade de controlo a nível nacional, a definição do montante mínimo das coimas consoante o tipo de empresa e o tipo de contraordenação. A revisão do montante máximo das coimas, também tendo em consideração o tipo de empresa e de contraordenação. Mantém-se a aplicação do valor que for mais elevado entre o montante máximo revisto e a percentagem do volume de negócio anual, conforme descrito na tabela abaixo.

Tipo empresa	**Tipo de contraordenação**			
	Muito grave		**grave**	
	Montante	**% do volume de negócio anual**	**Montante**	**% do volume de negócio anual**
Grande empresa	De € 5000 a € 20 000 000	4	De € 2500 a € 10 000 000	2
PME	De € 2000 a € 2 000 000	4	De € 1000 a € 1 000 000	2
Pessoas singulares	De € 1000 a € 500 000	-	De € 500 a € 250 000	-

Tabela 2.2 - Legislação nacional valores das coimas

Para as PME, os valores máximos tornam-se significativamente menores do que é definido por omissão pelo regulamento, no entanto continuam a ser valores que podem impactar o

funcionamento das empresas. A CNPD, de acordo com o artigo 39º da lei nº 58/2019, para além dos critérios estabelecidos no n.º 2 do artigo 83.º do RGPD, terá que ter em consideração os seguintes critérios para determinar o montante a aplicar:

a) A situação económica do agente, no caso de pessoa singular, ou o volume de negócios e o balanço anual, no caso de pessoa coletiva ;
b) O caráter continuado da infração ;
c) A dimensão da entidade, tendo em conta o número de trabalhadores e a natureza dos serviços prestados ;

Será necessário aguardar as primeiras atuações para perceber se as coimas aplicadas pela CNPD estarão mais próximas dos valores mínimos, assumindo assim uma postura mais benevolente, ou se estarão mais próximas dos valores máximos, servindo como exemplo da severidade do não cumprimento do regulamento. É também de destacar que o montante das coimas que forem aplicadas reverte 60% para o Estado e 40% para a CNPD.

3. PME

De acordo com a recomendação da comissão europeia de 6 de maio de 2013, PME são empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros (Europeia, 2006).

Existem 3 segmentações dentro das PME: micro, pequena e média empresa. Esta segmentação é feita de acordo com o número de colaboradores e pelo volume de negócios anual. A tabela abaixo apresenta os valores:

Definição	Número de pessoas que emprega	Volume de negócios anual
Microempresa	< 10	< 2 milhões de euros
Pequena empresa	< 50	< 10 milhões de euros
Média empresa	< 250	< 50 milhões de euros Ou balanço total anual inferior a 43 milhões de euros

Tabela 3.1 – Definição de PME

3.1. PME em Portugal

Segundo dados do INE (INE, 2019), em 2017 existiam 1.259.234 PME em Portugal. Este número representa 99.9% do tecido empresarial português e empregam um total de 3.114.405 de pessoas, cerca de 78.1% do emprego em Portugal, gerando uma faturação total de pouco mais de 225 mil milhões de euros.

De destacar também que do total de PME, 96,25% são microempresas, 3,22% são pequenas empresas e apenas 0,53% são médias empresas.

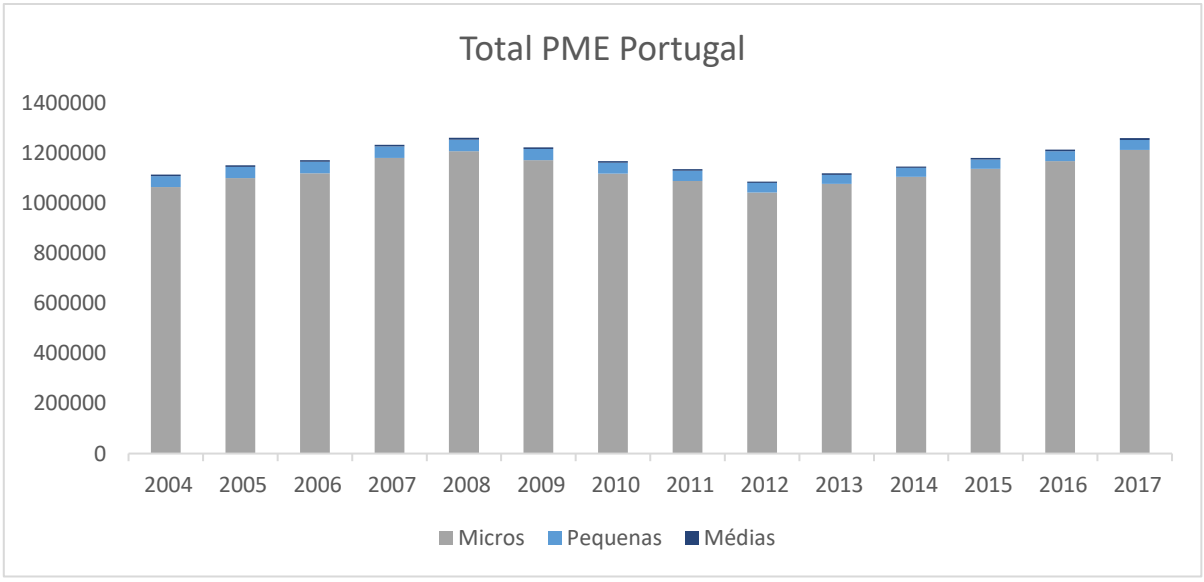

Figura 3.1 – Total de PME em Portugal

De notar também o efeito que a crise de 2008 teve no número de PME, que em 2012 reduziu cerca de 14% face ao máximo de 2008. O cenário está a reverter-se desde 2013 sendo que o número de PME volta a estar muito próximo do máximo de 2008, com uma taxa de crescimento de 3% ao ano em média.

Em termos de distribuição pelo país, nas regiões Norte e Grande Lisboa encontram-se 62% de todas as PME. Tem se notado nos últimos anos um aumento do número de PME nas restantes regiões do país, no entanto, é nestas 2 regiões onde são gerados 64% dos empregos remunerados e 65% do volume de negócios das PME.

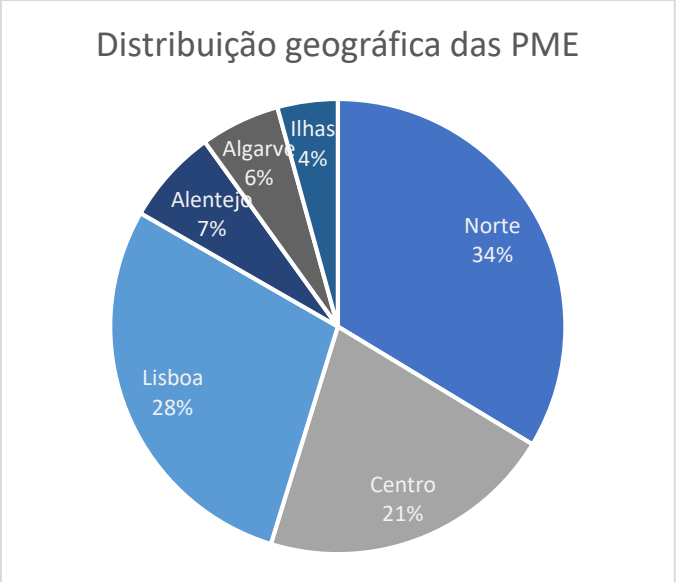

Figura 3.2 – Total de PME por região em Portugal

Dentro das PME, os setores com maior expressão são o Comércio por grosso e a retalho (17,4%), Agricultura, produção animal, caça, silvicultura e pesca (10,6%) e Alojamento, restauração e similares (8,3%). O setor de atividades imobiliárias, desde 2014, tem tido altas taxas de crescimento. Em 2017 registou uma variação positiva de 14% face ao ano anterior.

3.2. Desafio Digital

Entre muitos desafios que as PME enfrentam no seu dia-a-dia, tais como acesso ao crédito, carga fiscal pesada, legislação laboral e problemas de liquidez (Europeia, 2015), um desafio que se torna cada vez mais presente é ter uma estratégia digital (Fernandes, 2017).

De acordo com o estudo da ACEPI (ACEPI, 2018), em Portugal, todos os anos aumenta a percentagem da população que utiliza a internet e que faz compras online. Em 2018, 76% da população portuguesa utilizava a internet e 38% fizeram compras online. Os valores do comércio eletrónico (B2B[5] + B2C[6]) em Portugal ultrapassaram os 74,6 mil milhões de euros, representando um total de 40,6% do PIB nacional. Sendo que as previsões para 2025 apontam para que o comércio eletrónico representará 66,7% do PIB.

[5] Business to Business
[6] Business to Consumer

Apesar de se notar um aumento ao longo dos últimos anos, em 2018, apenas 37.3% do total das empresas portuguesas estavam presentes na internet. Se considerarmos apenas as PME, as empresas de maior dimensão apostam mais na presença online enquanto que as microempresas têm uma presença abaixo da média.

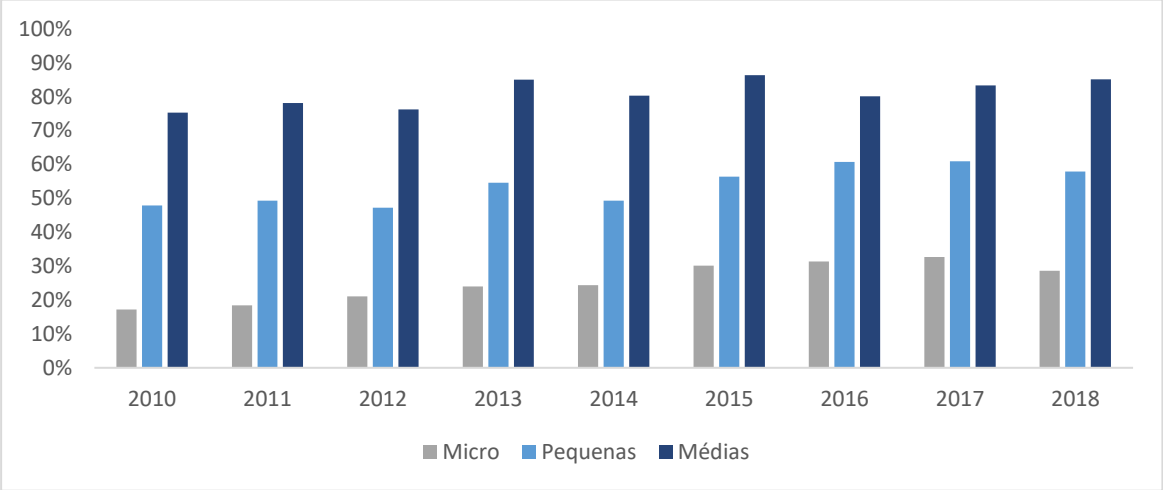

Figura 3.3 – Empresas com presença na internet por dimensão[7]

Este poderá ser um dos fatores que justifique que 90% dos portugueses recorre a sites estrangeiros para realizar compras online (ACEPI, 2018). As PME não podem considerar que o único fator de decisão do consumidor é o preço mais baixo dos concorrentes estrangeiros. Existem mais valias que estão mais ao alcance de uma empresa local, tais como o serviço de pós-venda, o aconselhamento na hora da compra e até mesmo os comentários de outros consumidores. Mas para isso a empresa tem que conhecer os seus consumidores e dar-se a conhecer ao mundo.

Uma estratégia digital passa por conhecer os consumidores, o mercado e as tendências (através de estudos analíticos como Business Intelligence e Big Data), identificar oportunidades e divulgar através de um Marketing Digital, de forma personalizada.

Esta será uma tendência natural para que as empresas tenham sucesso num mercado cada vez mais global, em que as fronteiras geográficas praticamente não existem. Em Portugal, 71% das PME consideram importante ter uma estratégia de marketing digital e social (Fernandes, 2017).

Neste percurso evolucionário, as empresas irão se deparar com o tratamento de dados pessoais, quer na fase de análise do negócio quer na divulgação de oferta e serviços. Por exemplo, muitas vezes o marketing digital é deixado a cargo de empresas de outsourcing. Com a implementação do RGPD, as empresas responsáveis pelo tratamento dos dados terão que assegurar a proteção dos dados pessoais mesmo quando estes estão a ser tratados por estas entidades externas, subcontratantes. Terão também que comunicar e garantir o consentimento do titular dos dados sempre que aplicável.

[7] Fonte: Pordata, 2018

4. DESCRIÇÃO DO ESTUDO REALIZADO

4.1. METODOLOGIA

Os resultados que serão apresentados foram com base em dados recolhidos através de um inquérito online divulgado, de forma gradual, através do e-mail de aluno da Nova IMS, entre os dias 19 de junho e 05 de julho de 2019, para 400 mil empresas.

No e-mail, as empresas tinham acesso a um link específico para o inquérito, alojado nos serviços do Google Form. Desta forma, a confidencialidade e a proteção dos dados das empresas foram garantidos uma vez que não existe registo de quem respondeu ao inquérito e nenhuma empresa é identificável através dos dados obtidos.

O inquérito esteve disponível até ao dia 19 de julho e foram obtidas 780 respostas, ou seja, uma taxa de resposta de aproximadamente 0,2%. No entanto, 18 inquiridos responderam que a dimensão da empresa é superior a 250 funcionários, o que não se enquadra numa das definições de PME, e por esta razão, foram excluídos da análise, reduzindo a dimensão da amostra para 762 PME.

Sobre os dados recolhidos, foi feita uma análise estatística descritiva, através das aplicações Excel e Power BI, cujos resultados serão apresentados de seguida.

4.2. CARACTERIZAÇÃO DAS PME DA AMOSTRA

A caraterização das empresas participantes é feita com base na idade, setor de atividade e dimensão. Também e feita uma caracterização da função que o inquirido exerce na empresa.

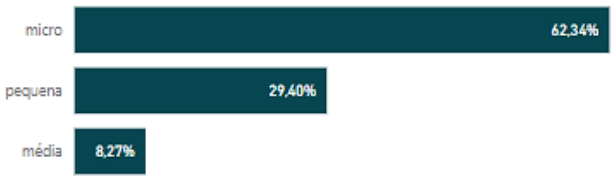

Figura 4.1 – Distribuição das PME por dimensão

Mais de metade das PME (62,34%) que responderam ao inquérito são microempresas (1-9 funcionários).

Figura 4.2 – Distribuição das PME por antiguidade

A maioria das PME que responderam ao inquérito (96.45%) estão no mercado a mais de 5 anos. O número reduzido de empresa com menos de 5 anos poderá estar relacionado com a antiguidade e pouca atualização da Base de Dados utilizada na divulgação do inquérito.

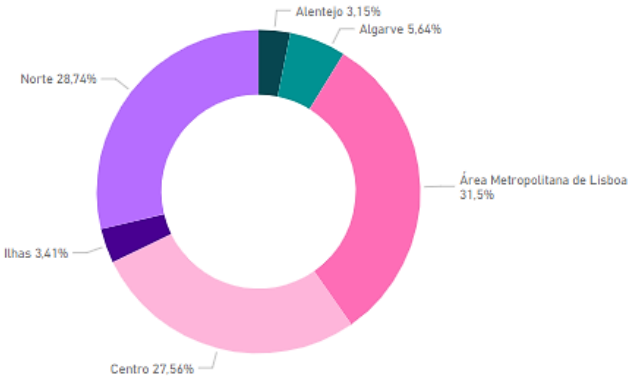

Figura 4.3 – Distribuição das PME por região

As PME que responderam ao inquérito estão mais concentradas nas regiões de Lisboa (31,5%), Norte (28,74%) e Centro (27,56%).

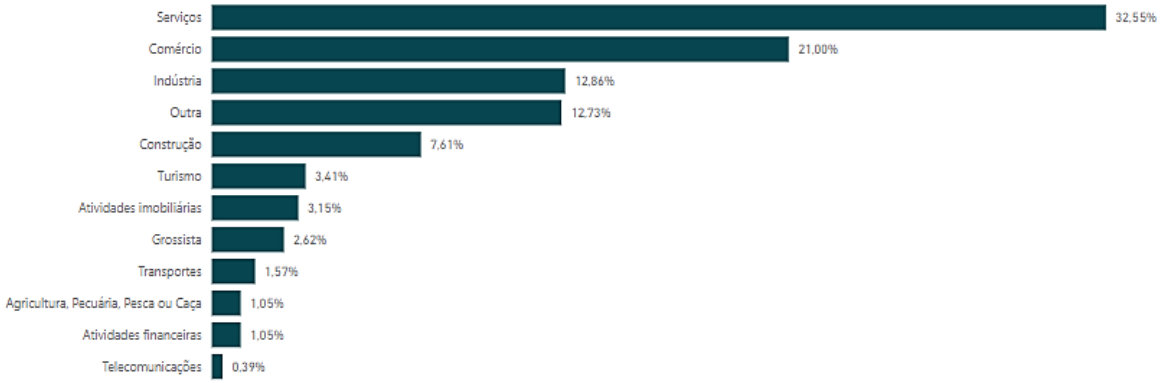

Figura 4.4 – Distribuição das PME por setor de atividade

Os setores mais representativos da amostra de PME são os Serviços (32,55%), o Comércio (21%) e a Industria (12,86%).

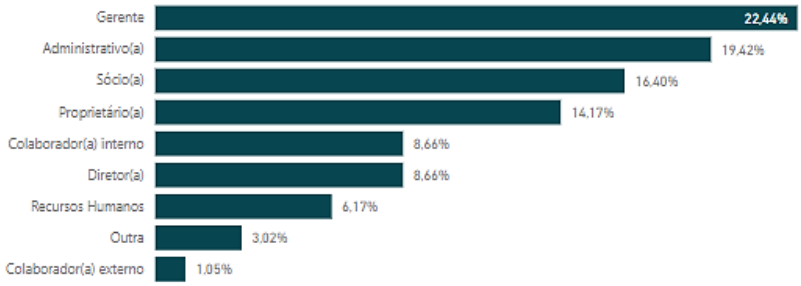

Figura 4.5 – Função do inquirido na PME

A maioria das pessoas que responderam ao inquérito em nome da PME assumem cargos que são considerados de topo, como Proprietário (14,17%), Sócio (16,4%) e Gerente (22,44%).

4.3. CONHECIMENTO DO RGPD

Foi questionado às empresas quando tiveram conhecimento do RGPD. Pouco mais de metade dos inquiridos responderam que só tiveram conhecimento do regulamento em 2018. Mesmo que este conhecimento tenha sido anterior à data de entrada em vigor do regulamento, 25 de maio de 2018, para algumas empresas terá sido difícil, se não impossível, implementar todas as alterações que o regulamento exige quer a nível dos sistemas de informação, quer a nível de procedimentos e formações das pessoas num espaço inferior a 3 meses. Conhecimentos posteriores a esta data implicaram sérios riscos de incumprimento.

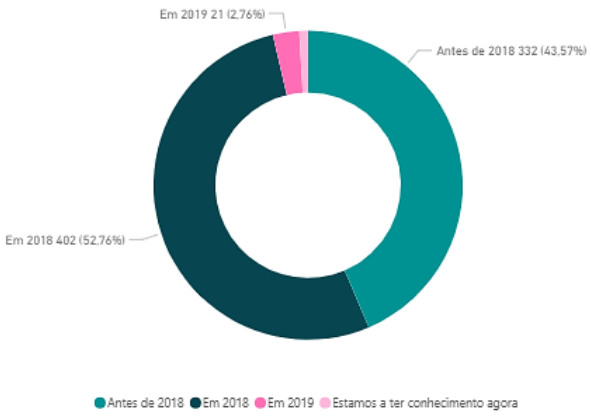

Figura 4.6 – Aquisição do conhecimento do RGPD

É também notório que as micro empresas foram as que tiveram o conhecimento mais tardio, inclusive sendo as únicas que referiram que o primeiro contato com o regulamento foi através deste inquérito.

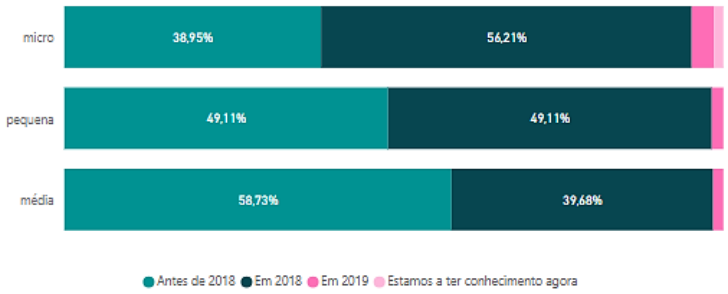

Figura 4.7 – Aquisição do conhecimento do RGPD por dimensão

Apesar de em muitos casos o conhecimento ter sido obtido tardiamente, mais de metade dos inquiridos consideram ter um bom ou muito bom nível de conhecimento sobre o regulamento.

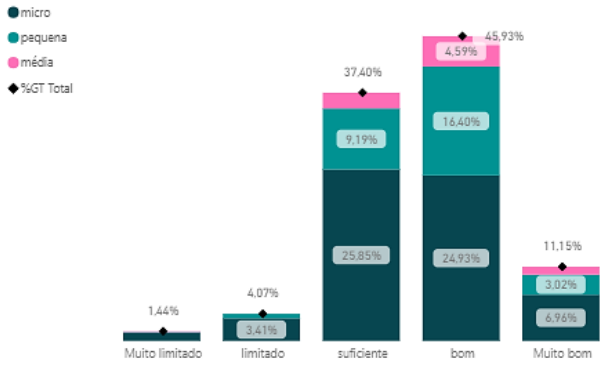

Figura 4.8 – Nível de conhecimento do RGPD

4.4. TIPO DE DADOS PESSOAIS E AQUISIÇÃO

Não seria possível num inquérito listar todos os tipos de dados pessoais que existem. Desta forma, foram apresentadas 11 categorias de dados aos inquiridos que poderiam escolher uma ou mais opões que se enquadrassem com o tratamento que a empresa efetua. Algumas das categorias podem conter um ou mais tipos de dados considerados especiais e que por isso poderão requerer maior cuidado no tratamento se este for lícito.

Categoria	Exemplos	Dados especiais
Identificação	nome, foto, dados biométricos	Sim
Médica e Saúde	tipo de sangue, DNA, resultados de testes, deficiências, prescrições e histórico clínico	Sim
Sociais	carreira académica ou profissional, salário, estrutura familiar, redes sociais	Não
Rastreamento	endereço IP ou MAC, email, número de telefone, localização, morada	Não
Financeiras	número de cartão de crédito, número de conta bancária, propriedades, transações (vendas, créditos, hábitos de compras)	Não
Características Físicas	altura, peso, idade, cor do cabelo, pele, tatuagens e género	Não
Autenticação	senhas de acesso, PIN, impressão digital	Não
Etnia	raça, origem e idiomas faladas	Sim
Sexual	vida sexual, preferências pessoais	Sim
Conhecimento e Crenças	crenças religiosas, filosóficas e pensamentos	Sim
Outro(s)		Talvez

Tabela 4.1 - Tabela categorias de dados pessoais

A categoria de identificação é, claramente, a mais utilizada pelas empresas. 72,5% selecionaram esta categoria como sendo uma das que possuem dados para tratamento.

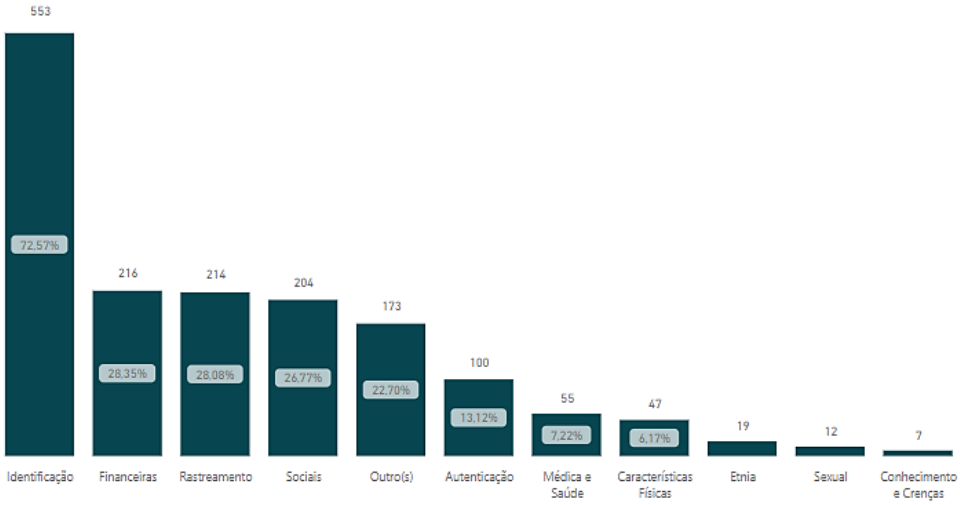

Figura 4.9 – Categoria de dados alvo de tratamento

Um dos exemplos de tipo de dados associados a categoria de identificação são os dados biométricos, que entram na categoria de dados especiais (artigo 9º). As empresas que selecionaram esta categoria, tendo em conta o tratamento deste tipo de dado, têm que ser capazes de comprovar que o tratamento é lícito, caso contrario entram em incumprimento.

As empresas podem efetuar tratamento de dados de mais do que um tipo de categoria, por exemplo, identificação e financeira.

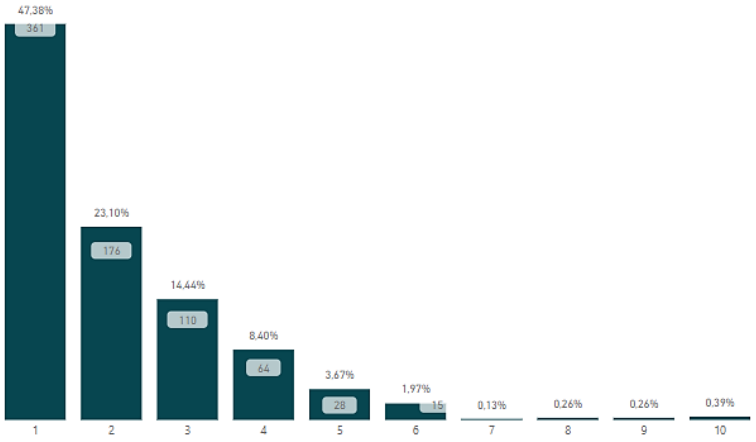

Figura 4.10 – Quantidade de categorias de dados pessoais

Neste inquérito, cerca de 47% das empresas identificaram apenas 1 tipo de categoria onde efetuam tratamento de dados.

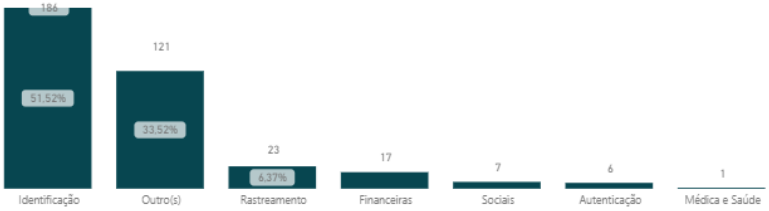

Figura 4.11 – Categorias de dados pessoais únicas

A categoria de identificação mantém-se como a principal (51,5%), dentro das empresas que responderam que efetuam tratamento de apenas 1 tipo de categoria de dados pessoais. Seguida por outro(s) (33,5%) e Rastreamento.

Apesar de ser possível, é pouco provável que uma empresa efetue apenas o tratamento de uma das categorias apresentadas. Basta pensar na gestão dos recursos humanos, que praticamente todas as empresas com mais do que um funcionário têm que fazer, implica o tratamento de, pelo menos, dados de identificação (nome e foto), sociais (salário), rastreamento (mail, telefone) e financeira (conta bancária). Observando o tipo de setor das empresas que disseram que só efetuam tratamento de um tipo de categoria de dados, o comércio, serviços e industria foram os que se destacaram.

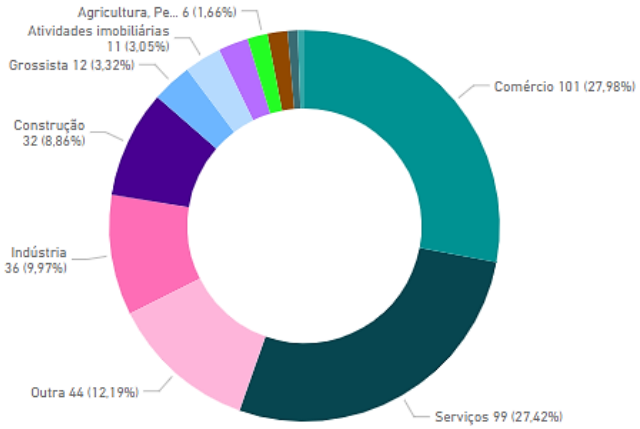

Figura 4.12 – Setores com tratamento de 1 categoria de dados pessoais

A análise destes dados sugere que poderá existir uma dificuldade das empresas em identificar o que são dados pessoais, com base no artigo 4º do RGPD, nomeadamente, no que diz respeito a um dado que torna uma pessoa identificável. Também pode indiciar que as empresas não estão a considerar os dados dos seus colaboradores como estando dentro do âmbito do regulamento.

Em relação à forma como os dados pessoais são obtidos, 75,59% responderam que uma das formas de obtenção é através de formulários presenciais, sendo o e-mail a segunda forma mais utilizada com 44,23%

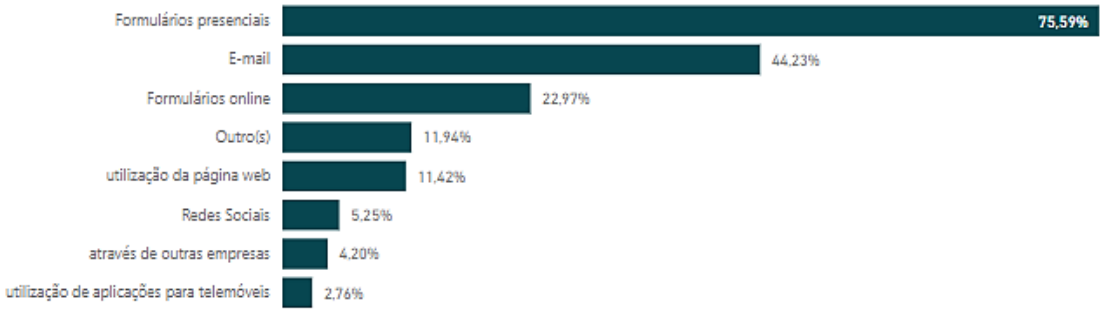

Figura 4.13 – Formas de aquisição dos dados pessoais

4.5. FINALIDADES E LICITUDE

Para cada finalidade de tratamento de um tipo de dado pessoal, com base no Artigo 30º do RGPD, a empresa tem que ser capaz de provar o que torna este tratamento lícito. No limite o consentimento do titular é uma das formas de legitimar este tratamento.

A CNPD (CNPD, s.d.),de forma a facilitar o cumprimento desta obrigação e referindo principalmente as PME, disponibiliza no seu site[8] um modelo para registo das atividades. É de destacar o ponto 4 do tratamento, em que é feita a associação da finalidade do tratamento, às categorias de dados tratado, as categorias dos titulares dos dados e o fundamento de licitude para este tratamento.

# tratamento	Qual a finalidade	Categorias de Dados tratados				Categorias dos		Fundamento de Licitude
		dados de identificação		dados de contacto		Recursos Humanos	Clientes	
		Dados	prazo de conservação	Dados	prazo de conservação			
T000	*ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade*	*ex: nome, fotografia, número de identificação civil*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: morada, e-mail, telefone*	*ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual*	*ex: sim*	*ex: sim*	*ex: Consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúd, interesse público ou exercício de autoridade pública*

Figura 4.14 – registo de tratamento modelo CNPD resumido

No inquérito realizado, 68,24% das PME disseram que uma das finalidades para tratamento é a Gestão de Clientes e Prestação de serviços, seguidos de Gestão Contabilística, fiscal e Administrativa com 51,05% e Cumprimentos de Obrigações legais com 50,39%

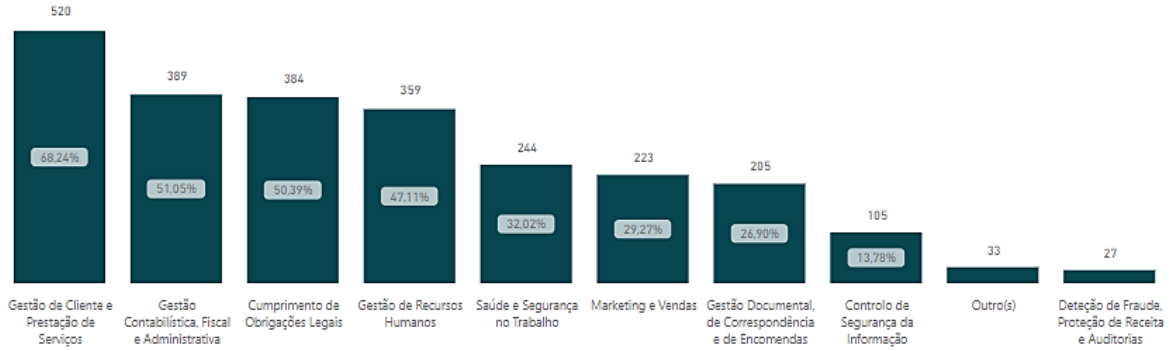

Figura 4.15 – Finalidades para o tratamento de dados

Sendo que os três principais fundamentos de licitude apontados foram: Cumprimento de Obrigações Legais (69,29%), Consentimento do Titular dos dados (55,25%) e Execução de contrato com o Titular dos dados (44,88%)

[8] https://www.cnpd.pt/bin/rgpd/docs/templateDocRGPD_resp_v1.xlsx

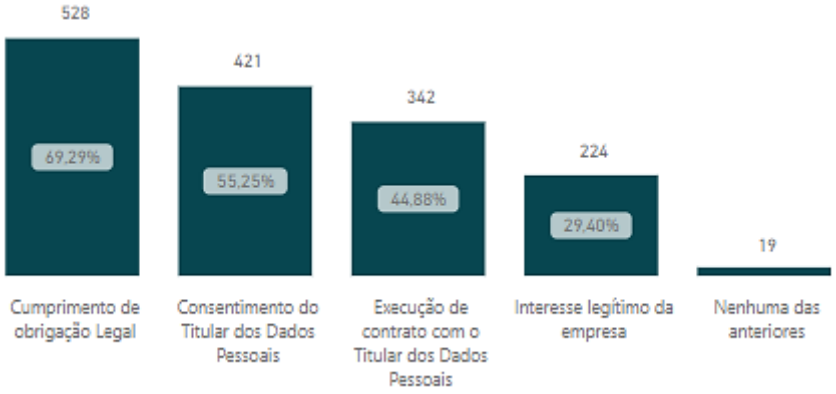

Figura 4.16 – Fundamentos de Licitude para o tratamento de dados

A licitude de uma finalidade não é algo linear, dependendo do contexto da empresa, a mesma categoria de finalidade pode ter fundamentos de licitude diferentes. No entanto, a finalidade de Marketing e Vendas é a única que pode ser feita uma associação direta com o consentimento do titular dos dados, já que nenhum outro fundamento é aplicável. Dos inquiridos que responderam que efetuam tratamento de dados com a finalidade de Marketing e Vendas, 71,75% assinalaram que um dos fundamentos da empresa é o Consentimento do titular.

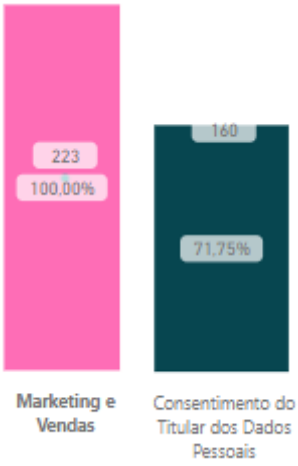

Figura 4.17 – Marketing e Vendas com consentimento

Estes dados não indicam que todos os 71,75% que têm como finalidade tratar os dados para ações de Marketing e Vendas usam como fundamento o Consentimento do Titular dos dados, no entanto indica que os restantes 28,25% estão a efetuar estas ações sem ter o consentimento do titular dos dados, o que torna o tratamento ilícito.

Quando questionadas se conseguiam provar que o tratamento dos dados é feito de forma lícita, mais de 70% disseram que concordam.

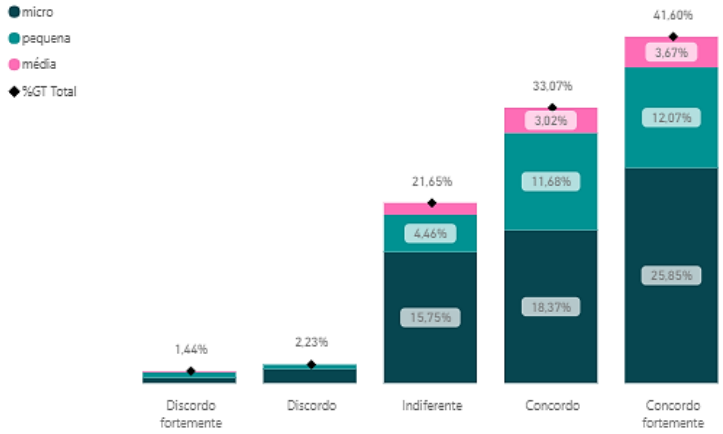

Figura 4.18 – Prova de tratamento lícito

4.6. ADAPTAÇÃO

Um dos primeiros passos que as empresas devem tomar para cumprir com o regulamento é fazer uma auditoria aos dados pessoais que detêm. Só desta forma conseguirão determinar as finalidades e as licitudes para o tratamento. Quando questionados se foi feita essa auditoria, 74,15% dos inquiridos responderam que não.

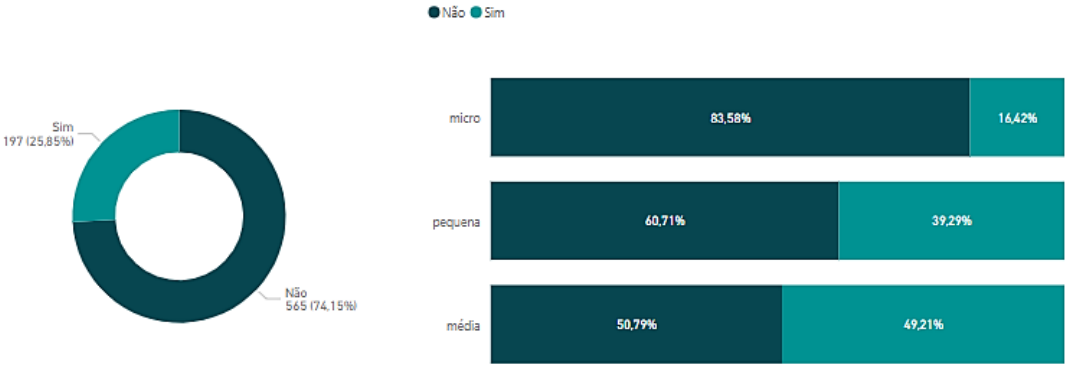

Figura 4.19 – Auditoria aos dados pessoais

As microempresas são as que apresentam uma tendência maior para não efetuarem esta auditoria.

Quando questionadas quais as principais dificuldades que tiveram na implementação do RGPD nas empresas, 46,06% indicaram a falta de conhecimento sobre o RGPD, 23,23% a falta de Recursos Humanos e 22,31% a incapacidade de identificar se os dados são alvo de um tratamento lícito.

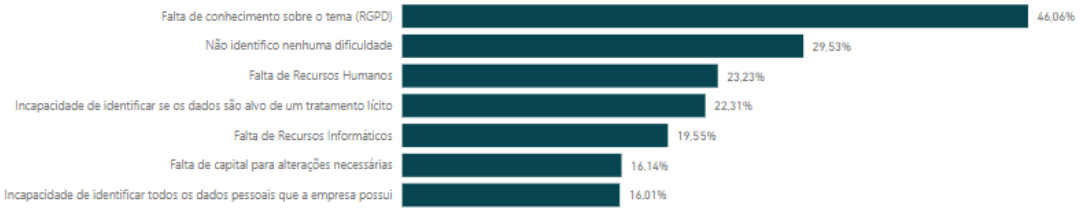

Figura 4.20 – Dificuldades em implementar o RGPD

Um fator que desperta atenção é que 29,53% não identificaram nenhuma dificuldade. Por ser um regulamento extenso e com vários pormenores, não era espectável um resultado tão elevado antes do inquérito. Seria interessante perceber se não ter identificado dificuldades significa que não acham que o RGPD se aplique a sua empresa ou se, por outro lado, implementaram medidas simples e suficientes para o cumprimento.

Procurou-se saber que ações foram tomadas para implementar o regulamento, sendo apresentadas as seguintes ações possíveis:

Ação	Explicação
Alteração de Procedimentos Internos	Alteração na forma como o trabalho é feito, novos cuidados a ter no tratamento de dados pessoais
Formação	Se foi apresentado aos colaboradores o novo regulamento e de que forma estes devem atuar
Alteração em SI	Alterações efetuadas em sistemas informáticos para cumprir o regulamento

Tabela 4.2 - Tabela ações tomadas

A maioria dos inquiridos adotou uma ou mais medida, sendo que a alteração dos procedimentos internos foi a mais utilizada.

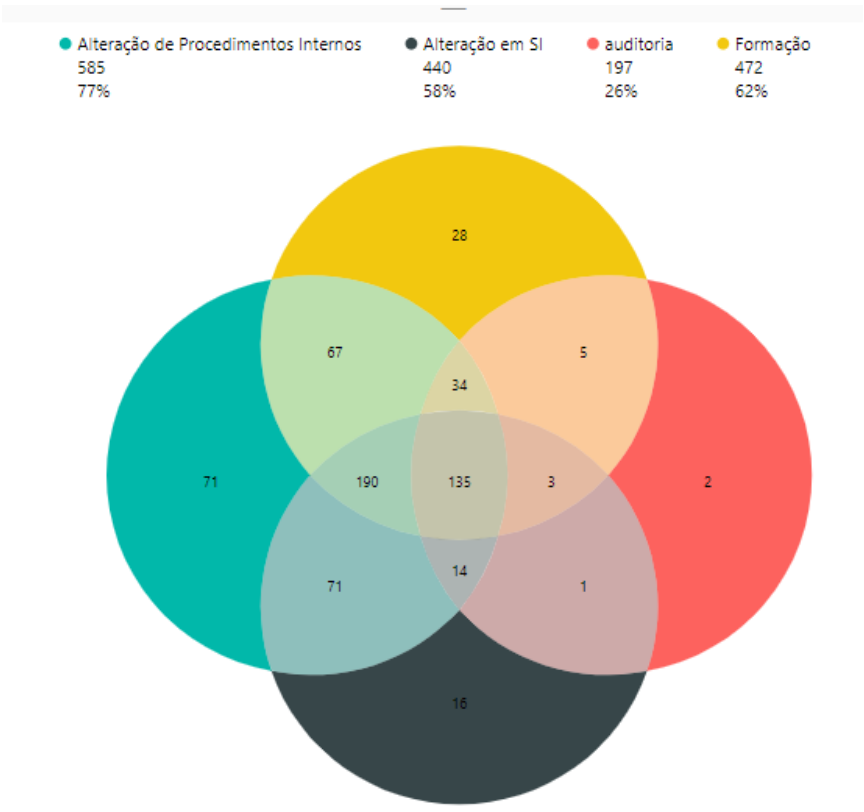

Figura 4.21 – Ações tomadas para implementar o RGPD

De destacar que 14,69% dos inquiridos não tomaram qualquer medida apresentada. Ou seja, não fizeram qualquer tipo de inventariado, não foi feita nenhuma alteração dos procedimentos internos,

não foi dada qualquer formação e também não foram alterados os sistemas informáticos. Mesmo assim, 67% dessas PME que não tomaram qualquer medida, afirmaram ser fácil para um titular de dados pessoais saber de que forma os seus dados estão a ser utilizados pela empresa.

Foi questionado também, que medidas foram tomadas em relação aos dados pessoais que a empresa já possuía antes do regulamento. 62,34% das empresas pediram consentimento ao titular dos dados, 23,62% apagaram alguns dados e 15,49% optaram por fazer a anonimização dos mesmos.

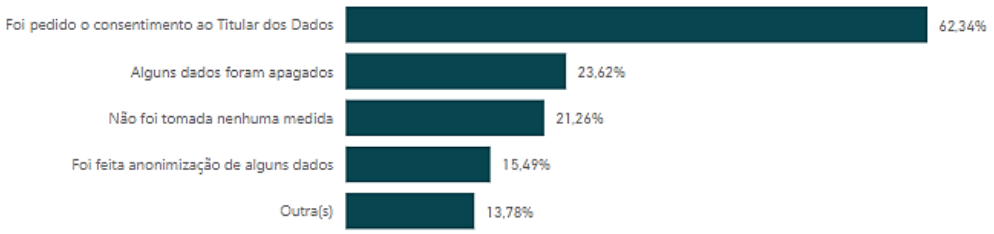

Figura 4.22 – Ações tomadas sobre dados antes do RGPD

Ao serem questionadas se estão preocupadas com a possibilidade de serem multadas por incumprimento do regulamento, apenas cerca de 20% das PME demonstram algum tipo de preocupação.

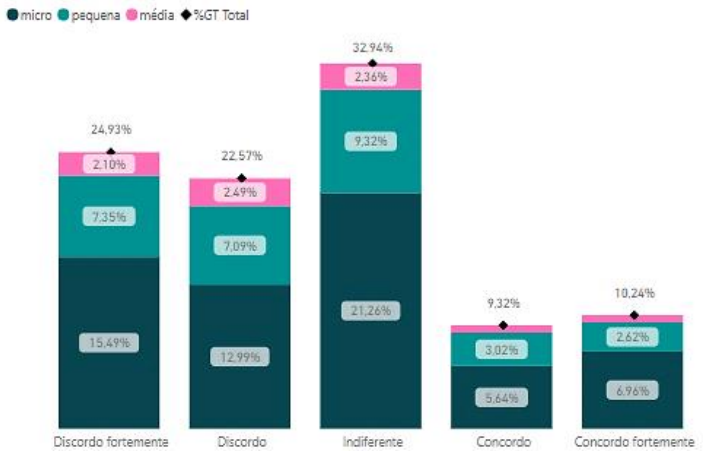

Figura 4.23 – Receio de multa por incumprimento do RGDP

Esta falta de preocupação poderá ser consequência na demora da implementação de uma legislação nacional e também pelo fato de após 1 ano de implementação do RGPD, o número de coimas aplicadas em Portugal, ao abrigo do RGPD, ter sido bastante reduzido. Poderá existir um sentimento de falta de controlo e até mesmo, tal como reportado no relatório da GDPR.eu (GDPR.eu, 2019), a sensação de que eventuais multas não serão direcionadas às PME, mas sim as grandes corporações e instituições públicas.

4.7. DIREITOS DE ACESSO E ESQUECIMENTO

As PME terão que ser capazes de responder a todos os direitos de um titular de dados, no entanto, nesta dissertação foi dado um foco maior a estes dois direitos, direito de acesso e de esquecimento,

pois deverão ser os mais solicitados pelos titulares de dados pessoais e têm uma relação direta quando o tratamento é feito com base no consentimento.

Foi questionado se é fácil para um titular de dados pessoais saber de que forma os seus dados estão a ser utilizados pela empresa. 75.73% concordaram ou concordaram fortemente que é fácil o acesso a esta informação.

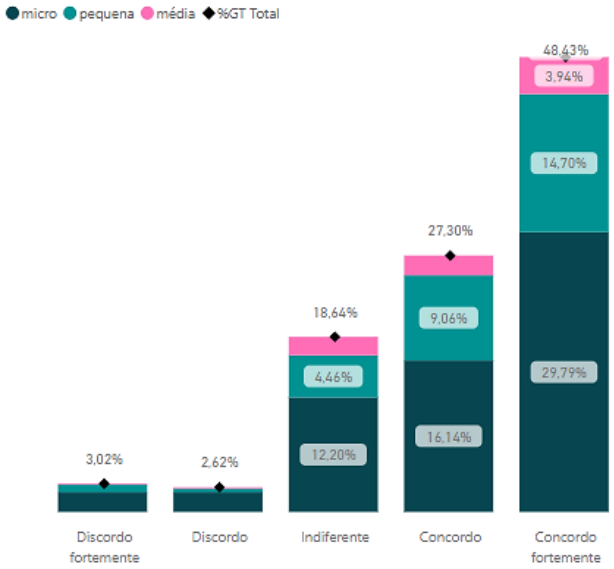

Figura 4.24 – Facilidade de acesso aos dados

Em relação a quanto tempo demora a ser passada esta informação ao titular dos dados pessoais, as empresas responderam, maioritariamente, que em 15 dias a informação é disponibilizada. Sendo que existem micro e pequenas empresas que responderam que não conseguem prestar a informação de como os dados são utilizados.

Figura 4.25 – Tempo que demora a prestar a informação da utilização dos dados pessoais

Foi também questionado se é fácil para um titular de dados pessoais saber como pode pedir o apagamento dos seus dados pessoais. 75.81% concordaram ou concordaram fortemente que é fácil obter esta informação.

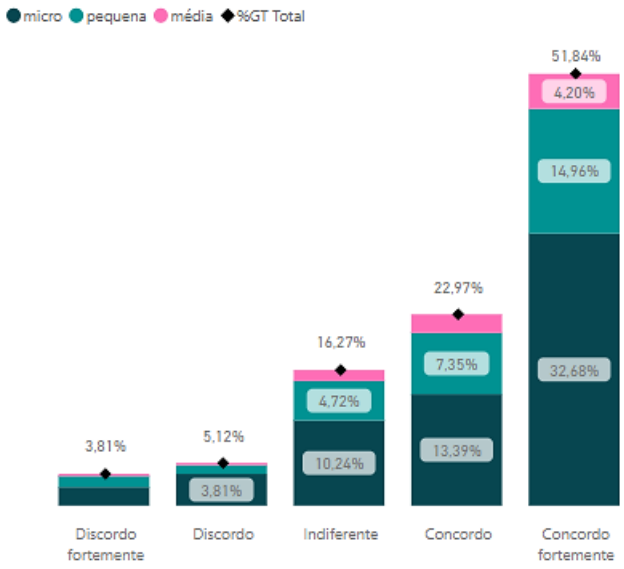

Figura 4.26 – Facilidade de pedido de esquecimento

Em relação ao tempo que a empresa considera que demora a apagar os dados pessoais de um titular após um pedido de apagamento, a maioria das empresas indicam que num prazo de 15 dias os dados são apagados. No entanto, é possível observar que com o aumento da dimensão da empresa, aumentam também os períodos que demoram a apagar, sendo que 30,16% das médias empresas chegam mesmo a indicar que não conseguem precisar o tempo que demoram, tendo que ser avaliado.

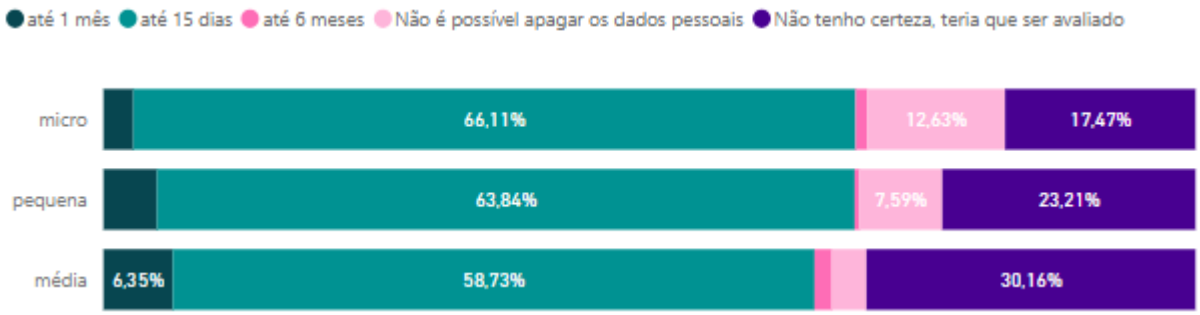

Figura 4.27 – Tempo que demora a apagar os dados pessoais

5. **CONCLUSÕES**

O Regulamento Geral sobre a Proteção de Dados (RGPD) em suma:

- Altera o paradigma de ação de uma lógica de Deteção e Correção para uma lógica de Prevenção;
- Pressupõe um caminho de melhoria contínua na proteção dos Dados Pessoais ;
- Cria um contexto de maior consciencialização e preocupação por parte dos cidadãos sobre a proteção dos seus Dados Pessoais;
- Reforça os poderes das autoridades de controlo para investigar e inspecionar o cumprimento;
- Aumenta os impactos de não cumprimento para o negócio, desde as penalizações financeiras aos danos na reputação;
- Passa a responsabilidade de cumprimento para as empresas e para cada um de nós que tratamos Dados Pessoais;

Neste trabalho, foi possível identificar que a maioria das PME portuguesas (96,3%) têm conhecimento do que é o RGDP. Sendo que 52,7% só tiveram conhecimento em 2018, ano da entrada em vigor do regulamento.

Das 762 PME que participaram no inquérito, 47% identificam apenas uma categoria de dados pessoais como alvo de tratamento, sendo a categoria de identificação a principal, o que poderá sugerir que estão apenas a considerar os dados de clientes, ignorando dados pessoais de colaboradores e fornecedores, por exemplo.

As principais finalidades apontadas para tratamento de dados pessoais foram: a *Gestão de Clientes e Prestação de serviços*, *Gestão Contabilística, fiscal e Administrativa* e *Cumprimentos de Obrigações legais*. Sendo que os três principais fundamentos de licitude apontados foram: *Cumprimento de Obrigações Legais*, *Consentimento do Titular dos dados* e *Execução de contrato com o Titular dos dados*.

Ter uma estratégia digital tornou-se fundamental para o crescimento de qualquer empresa, inclusive para as PME. Esta estratégia passa por ações de Marketing Digital para que possam comunicar com os seus clientes de uma forma direta e personalizada. No entanto, isto implica o consentimento do titular. Das PME que referiram como uma das finalidades para tratamento de dados pessoais o Marketing e Venda, 28% não referiram o consentimento do titular como forma de tornar o tratamento lícito.

Apenas uma minoria das PME (25,85%) realizou uma auditoria aos dados que detêm. Apesar disso, 75,7% das empresas afirmam ser fácil para um titular de dados pessoais saber de que forma os seus dados estão a ser utilizados pela empresa e que conseguem prestar esta informação num prazo de 15 dias, quando solicitado.

Em relação às medidas que foram tomadas sobre os dados pessoais que as PME detinham antes do RGPD entrar em vigor, 62,34% pediram consentimento para o tratamento e 23,62% indicaram terem apagado alguns dados.

Algo surpreendente neste inquérito foi o facto de cerca de metade das PME (47,5%) não demonstrarem preocupação em serem multadas por incumprimento do regulamento. Apenas 20% das PME demonstraram algum tipo de preocupação, as restantes demonstraram um sentimento neutro.

A CNPD terá um papel fundamental no sucesso da implementação do regulamento pelas empresas, principalmente nas PME. Este órgão deverá auxiliar as empresas com a divulgação de orientações específicas aos diversos setores de atividade e com exemplos de dados pessoais. As coimas que vierem a ser aplicadas também poderão ser um fator decisivo para forçar o investimento das PME no cumprimento do regulamento.

6. LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Durante a fase de pesquisa, não foi possível encontrar trabalhos que relacionassem o RGPD com as PME, quer a nível nacional quer a nível europeu. A maioria das referências são artigos em páginas web e documentação própria da comissão europeia.

Neste inquérito, foi feita uma análise transversal e genérica a todos os tipos de PME. Tal impediu que fosse feita a associação direta entre categoria de dados pessoais, com as finalidades de tratamento e com o fundamento de licitude, uma vez que são relações complexas e que podem variar consoante o setor de atividade e características próprias de cada empresa.

Como trabalho futuro, poderá ser feita uma análise semelhante, mas para um setor de atividade específico, detalhando assim melhor os tipo de dados pessoais e os tratamentos associados a essa atividade, as finalidades e os fundamentos de licitude. Podendo assim inclusive, surgir recomendações específicas para que este setor possa implementar de forma correta o RGPD e até mesmo ser feita uma prova de conceito com uma PME.

Também poderá se explorar a vertente da continuidade da implementação do RGDP. Estarão as empresas, nomeadamente as PME, a investirb na proteção dos dados? Consideram que as medidas tomadas no passado foram suficientes? Pensam na proteção dos dados na implementação de novos processos e sistemas?

7. **BIBLIOGRAFIA**

ACEPI. (2018). *Estudo Economia Digital em Portugal-2018.*

Adebiyi, A., & Obasan, K. (2016). *Strategic Management and Small and Medium Enterprises (SMEs) Development: A Review of Literature.*

Albrecht, J. P. (2016). How The GDPR Will Change The World. Em *European Data Protection Law Review* (pp. 287-289).

Bygrave, L. A. (2003). *Digital Rights Management and Privacy – Legal Aspects in the European Union.*

Calvão, F. (17 de Maio de 2019). á houve quatro multas em Portugal por causa do RGPD. Uma foi ao Hospital do Barreiro e três a empresas privadas. (H. Amaral, Entrevistador) Obtido de https://eco.sapo.pt/2019/05/17/ja-houve-quatro-multas-em-portugal-por-causa-do-rgpd-uma-foi-ao-hospital-do-barreiro-e-tres-a-empresas-privadas/

CNPD. (s.d.). *Espaço RGPD*. Obtido de Comissão Nacional de Proteção de Dados: https://www.cnpd.pt/bin/rgpd/rgpd.htm

Constantinides, E. (2004). *Influencing the online consumer''s behaviour: the Web Experience.*

Devitt, A., Duffin, J., & Moloney, R. (2005). *Topographical Proximity for Mining Network Alarm Data.* Irland: Ericsson R&D.

Europeia, C. (2006). *Recomendação n.º 2003/361/CE relativa à definição de micro, pequenas e médias empresa.*

Europeia, C. (2015). *Report on the public consultation on the "New SME Policy".*

Europeia, C. (s.d.). *Orientações sobre os encarregados da proteção de dados (EPD).* Obtido de https://ec.europa.eu/info/law/law-topic/data-protection_en

Europeia, C. (s.d.). *Proteção de dados*. Obtido de Regras melhores para as pequenas empresas: https://ec.europa.eu/justice/smedataprotect/index_pt.htm

Fernandes, Z. (2017). *Retrato Digital das PME Portuguesas - 2017.* PSE.

GDPR.eu. (2019). *GDPR Small Business Survey.*

INE. (2019). *Empresas em Portugal - 2017.*

Jiahong, C. (2016). *International Data Privacy Law.*

Magalhães, F. M., & Pereira, M. L. (2018). *Regulamento Geral de Proteção de Dados - Manual Prático - 2ª Edição Revista e Ampliada.* Vida Economica Editorial.

Portugues, G. (s.d.). *Lei nº 58/2019 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 circ.* Diário da República.

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. (2016). *Jornal Oficial da União Europeia*.

Team, I. P. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide.* IT Governance Publishing.

8. **ANEXOS**

localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Tratamento

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;

2. **Efetua o tratamento de dados pessoais para que fins?** *
Escolher uma ou mais opções
Marque todas que se aplicam.

- [ ] Marketing e Vendas
- [ ] Gestão de Cliente e Prestação de Serviços
- [ ] Gestão Contabilística, Fiscal e Administrativa
- [ ] Deteção de Fraude, Proteção de Receita e Auditorias
- [ ] Cumprimento de Obrigações Legais
- [ ] Controlo de Segurança da Informação
- [ ] Gestão Documental, de Correspondência e de Encomendas
- [ ] Gestão de Recursos Humanos
- [ ] Saúde e Segurança no Trabalho
- [ ] Outro(s)

3. **Efetua o tratamento de que tipo de dados pessoais?** *
Escolher uma ou mais opções
Marque todas que se aplicam.

- [ ] Identificação: nome, foto, dados biométicos
- [ ] Características Físicas: altura, peso, idade, cor do cabelo, pele, tatuagens e género
- [ ] Etnia: raça, origem e idiomas faladas
- [ ] Sexual: vida sexual, preferências pessoais
- [ ] Conhecimento e Crenças: crenças religiosas, filosóficas e pensamentos
- [ ] Média e Saúde: tipo de sangue, DNA, resultados de testes, deficiências, prescirções e histórico clínico
- [ ] Financeiras: número de cartão de crédito, número de conta bancária, propriedades, transações (vendas, créditos, hábitos de compras)
- [ ] Sociais: carreira académica ou profissional, salário, estrutura familiar, redes sociais
- [ ] Rastreamento: endereço IP ou MAC, email, número de telefone, localização, morada
- [ ] Autenticação: senhas de acesso, PIN, impressão digital
- [ ] Outro(s)

4. **Considera que o tratamento dos dados pessoais é feito em que âmbito?** *
Escolher uma ou mais opções
Marque todas que se aplicam.

- [ ] Execução de contrato com o Titular dos Dados Pessoais
- [ ] Interesse legítimo da empresa
- [ ] Cumprimento de obrigação Legal
- [ ] Consentimento do Titular dos Dados Pessoais
- [ ] Nenhuma das anteriores

5. **Como classifica a quantidade de dados pessoais que detêm face ao que a empresa precisa?** *
Marcar apenas uma oval.

- ◯ Insuficiente
- ◯ Adequada
- ◯ Mais do que suficiente

6. **De que forma os dados são obtidos?** *
Marque todas que se aplicam.

- [ ] Formulários presenciais
- [ ] Formulários online
- [ ] E-mail
- [ ] Redes Sociais
- [ ] utilização da página web
- [ ] utilização de aplicações para telemóveis
- [ ] através de outras empresas
- [ ] Outro(s)

7. **Envia dados pessoais para empresas externas para tratamento de dados?** *
Por exemplo para empresas de marketing ou consultoras
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

8. **Ao enviar dados pessoais para uma empresa externa, considera que a responsabilidade sobre a proteção dos dados é da responsabilidade de quem?** *
Marcar apenas uma oval.

- ◯ Da minha empresa
- ◯ Da empresa parceira
- ◯ De ambas

Implementação

9. **Recorreu a algum serviço especializado para garantir o cumprimento do regulamento?** *
Exemplo: empresas externas ou consultores
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

10. **Foi feito algum inventário dos dados pessoais que a empresa detém?** *
identificação dos dados que possuem, quem tem acesso, onde estão localizados, por quanto tempo são retidos
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

11. **Sobre os dados pessoais que a empresa já detinha antes do RGPD, que medidas foram tomadas?** *
Escolher uma ou mais opções
Marque todas que se aplicam.

- ☐ Não foi tomada nenhuma medida
- ☐ Alguns dados foram apagados
- ☐ Foi pedido o consentimento ao Titular dos Dados
- ☐ Foi feita anonimização de alguns dados
- ☐ Outra(s)

12. **Foi feita alguma alteração nos sistemas informáticos para cumprir o regulamento?** *
Exemplos: mudanças na página de internet, registo de acessos, criação de perfis de utilizadores
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

13. **Foi feita alguma alteração nos procedimentos internos para cumprir o regulamento?** *
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

14. **Foi dada alguma formação/treino sobre a proteção de dados aos colaboradores da empresa?** *
Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

15. **A empresa consegue provar que os dados pessoais que detém são tratados de forma lícita** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	◯	◯	◯	◯	◯	Concordo fortemente

16. **Apenas pessoas autorizadas conseguem aceder aos dados pessoais** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	◯	◯	◯	◯	◯	Concordo fortemente

17. **É fácil para um titular de dados pessoais saber de que forma os seus dados estão a ser utilizados pela empresa** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	◯	◯	◯	◯	◯	Concordo fortemente

18. **É fácil para um titular de dados pessoais saber como pedir o apagamento dos seus dados pessoais** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	◯	◯	◯	◯	◯	Concordo totalmente

19. **Se um titular de dados pessoais pedir informação de como os seus dados estão a ser utilizados, em quanto tempo consegue prestar esta informação?** *
Marcar apenas uma oval.

- ◯ Não é possível prestar esta informação
- ◯ até 15 dias
- ◯ até 1 mês
- ◯ Até 6 meses
- ◯ Não tenho a certeza, teria que ser avaliado

20. **Se um titular de dados pessoais pedir para apagar os seus dados pessoais, em quanto tempo considera que os mesmos são apagados?** *
Marcar apenas uma oval.

- ◯ Não é possível apagar os dados pessoais
- ◯ até 15 dias
- ◯ até 1 mês
- ◯ até 6 meses
- ◯ Não tenho certeza, teria que ser avaliado

Dificuldades e receios

21. **Quais considera que são as 3 principais dificuldades que existem para o cumprimento do regulamento?** *

Marque todas que se aplicam.

- [ ] Falta de Recursos Humanos
- [ ] Falta de Recursos Informáticos
- [ ] Falta de conhecimento sobre o tema (RGPD)
- [ ] Falta de capital para alterações necessárias
- [ ] Incapacidade de identificar todos os dados pessoais que a empresa possui
- [ ] Incapacidade de identificar se os dados são alvo de um tratamento lícito
- [ ] Não identifico nenhuma dificuldade

22. **Estou preocupado com a possibilidade da empresa ser multada por incumprimento do regulamento** *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo fortemente	◯	◯	◯	◯	◯	Concordo fortemente

Perfil da empresa

23. **Quantos funcionários possui a empresa?** *

Marcar apenas uma oval.

- ◯ 0-9
- ◯ 10-49
- ◯ 50-249
- ◯ 250 ou mais

24. **Há quantos anos a empresa existe?** *

Marcar apenas uma oval.

- ◯ Menos de 1 ano
- ◯ 1-5 anos
- ◯ 6-19 anos
- ◯ 20 ou mais anos

25. **Qual o principal setor de atividade da empresa?** *
Marcar apenas uma oval.

- ◯ Agricultura, Pecuária, Pesca ou Caça
- ◯ Comércio
- ◯ Construção
- ◯ Atividades imobiliárias
- ◯ Indústria
- ◯ Serviços
- ◯ Transportes
- ◯ Turismo
- ◯ Grossista
- ◯ Telecomunicações
- ◯ Atividades financeiras
- ◯ Outra

26. **Qual a região do país onde se localiza a sede da empresa?** *
Marcar apenas uma oval.

- ◯ Norte
- ◯ Área Metropolitana de Lisboa
- ◯ Centro
- ◯ Alentejo
- ◯ Algarve
- ◯ Madeira
- ◯ Açores

Inquirido

27. **Qual a sua função na empresa?** *
Marcar apenas uma oval.

- ◯ Proprietário(a)
- ◯ Sócio(a)
- ◯ Gerente
- ◯ Diretor(a)
- ◯ Recursos Humanos
- ◯ Administrativo(a)
- ◯ Colaborador(a) interno
- ◯ Colaborador(a) externo
- ◯ Outra

28. **Qual o seu nível de conhecimento acerca do assunto do questionário? (RGPD)** *
Marcar apenas uma oval.

	1	2	3	4	5	
Muito limitado	⬭	⬭	⬭	⬭	⬭	Muito bom

29. **Qual o seu nível de conhecimento acerca da Nova IMS?** *
Marcar apenas uma oval.

	1	2	3	4	5	
Muito limitado	⬭	⬭	⬭	⬭	⬭	Muito bom