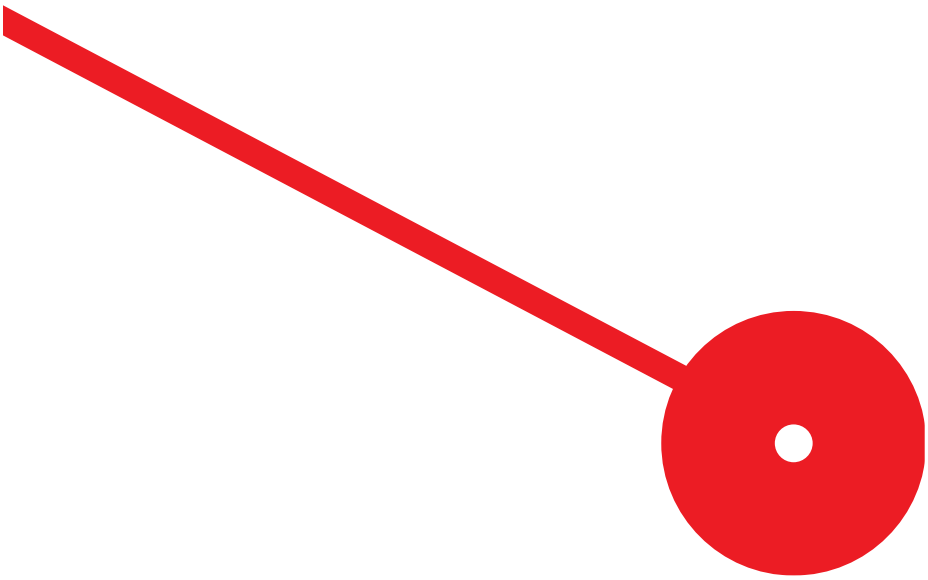
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
AUDITORIA

RGPD (Regulamento geral de proteção de dados): conhecimento e impacto nas organizações

Flávia Raquel Soares Machado

11/2020



Flávia Raquel Soares Machado
11/2020

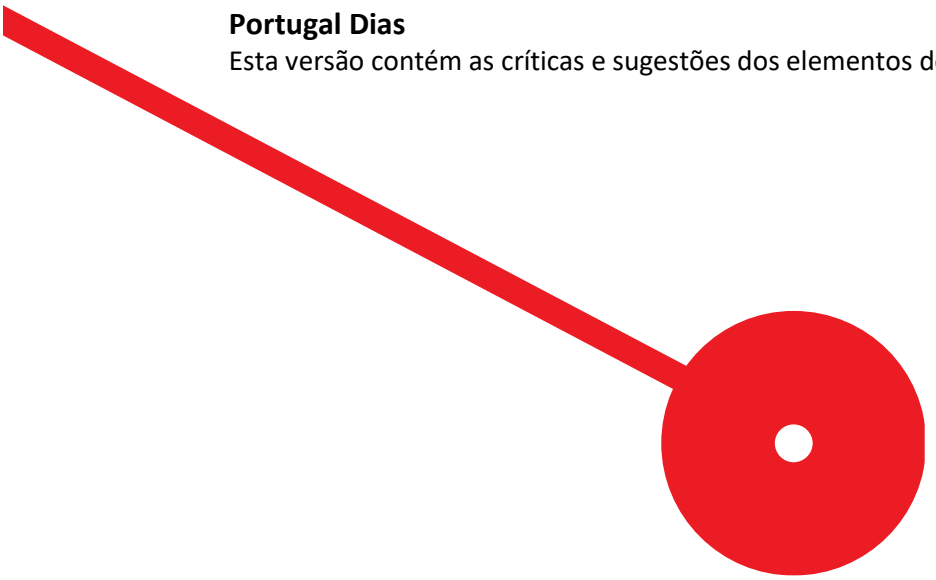
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
AUDITORIA

RGPD (Regulamento geral de proteção de dados): conhecimento e impacto nas organizações

Flávia Raquel Soares Machado

Dissertação de Mestrado
apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação de Exma. Professora Doutora Alcina Augusta de Sena Portugal Dias
Esta versão contém as críticas e sugestões dos elementos do júri



Flávia Raquel Soares Machado
11/2020

Resumo:

O Regulamento geral de proteção de dados (RGPD) é um diploma (2016/679) do parlamento europeu e do conselho de 27 de abril de 2016. Atualmente a Lei nacional de execução 58/2019 assegura o seu cumprimento na ordem jurídica nacional.

Este regulamento tem como objetivo primordial servir de reforço à proteção de dados respondendo à carta dos direitos fundamentais da UE e abrange qualquer pessoa singular ou coletiva, pública ou privada que trate de dados pessoais. Dada a livre circulação de pessoas e capitais, a crescente globalização e o avanço tecnológico, o fluxo de dados tornou-se descontrolado. Este regulamento visa assegurar a proteção de consequências negativas da livre circulação de dados na União Europeia.

O objetivo é obter ilações sobre o conhecimento e impacto do RGPD nas organizações. Apurar as implicações e constrangimentos que este trouxe e perceber o papel que assume o encarregado de proteção de dados neste âmbito. É ainda objetivo do estudo perceber o contributo das auditorias realizadas neste âmbito.

Para este efeito foi elaborado um questionário direcionado aos profissionais das empresas que compõe o PSI-20. O estudo contou ainda com uma pequena análise qualitativa feita através de pedido de opinião profissional sobre a temática.

As hipóteses em estudo foram comprovadas em 72%, em média, conforme demonstrado na análise dos resultados. Sendo que se concluiu que existe conhecimento do RGPD nas organizações, a aplicação do regime trouxe algum impacto percebido. O Encarregado de proteção de dados é uma figura conhecida, embora necessite de formação adicional. As auditorias realizadas neste âmbito traduzem-se em apoios positivos e fundamentais.

Palavras chave: RGPD, Proteção, Dados pessoais, Tratamento, Encarregado proteção dados

Abstract:

The General Data Protection Regulation (GDPR) is a legal document (2016/679) from the European Parliament and the Council of 27 April 2016. Currently, LNE 58/2019 ensures the implementation in the national legal order of the GDPR.

The primary objective of this regulation is to reinforce data protection by responding to the EU Charter of Fundamental Rights and covers any person or entity, public or private, dealing with personal data. Because of the free movement of people and capital, the increasing globalization and technological advancement, the data flow has become uncontrolled. This regulation ensures protection from negative consequences of free circulation of data in the EU.

The prupose is to learn about the perception and impact of GDPR on organizations. Understand the implications and constraints of the regulation and the position of the data protection Officer. It is also the objective of research to understand the contribution of audits carried out in this area.

For this purpose, a questionnaire was designed for professionals in the companies of the PSI-20. Additionally it was made a small qualitative analysis made through a professional opinion on the theme.

The hypotheses were proven in 72%, on average, as demonstrated in the analysis of the results. It was concluded that there is knowledge of GDPR in organizations, the application of the regime brought some perceived impact. The EPD is a well-known figure, although it needs additional professional training and the audits carried out in this area translate into positive support.

Key words: GDPR, Protection, Personal data, data protection officer

Agradecimentos

A conclusão da presente dissertação representa a fase final de um percurso académico a que me propus. Representa a realização de mais um objetivo, e não posso deixar de partilhar a conquista desta pequena meta pessoal com quem a viveu comigo.

Agradeço sobretudo aos meus pais e irmãos por todo o apoio incondicional, incentivo e orgulho que sempre demonstram a cada etapa concluída da minha vida.

Ao João, meu namorado, pela paciência, por me ajudar a manter o foco nas alturas mais difíceis e por todo o incentivo e compreensão.

Aos meus colegas de trabalho e amigos, pelas palavras de incentivo e por toda a solidariedade demonstrada.

À minha orientadora, Professora Doutora Alcina Portugal Dias pela disponibilidade, pelas recomendações, por toda ajuda e conselhos ao longo do percurso.

A todos profissionais que contribuíram gentilmente com a sua ajuda e saber, só assim foi possível a recolha dos dados necessários.

Um gigante obrigada a todos que me acompanharam durante esta etapa!

Lista de abreviaturas

ACT – Autoridade para as Condições do Trabalho

AEPD – Autoridade europeia para a proteção de dados

AI – Auditoria interna

AIPD – Avaliação de Impacto sobre a Proteção de Dados

AL. – Alínea

CdE – Conselho da Europa

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CE - Conselho Europeu

CEDH – Convenção Europeia dos Direitos do Homem

CNPD – Comissão nacional de proteção de dados

CRF - Confrontar

CRP – Constituição da República Portuguesa

CT – Código do trabalho

DL – Decreto Lei

DPO - Data Protection Officer

GT – Grupo de Trabalho

IAPP - International Association of Privacy Professionals

LNE – Lei Nacional de execução do RGPD

Nº - Número

PE – Parlamento Europeu

RGPD – Regulamento Geral de Proteção de Dados

RH – Recursos Humanos

UE – União Europeia

Índice geral

Índice de Figuras

Índice de Tabelas

As primeiras ações de processamento de dados em larga escala e de forma centralizada, foram no ano de 1960, por iniciativa dos Estados Unidos e alguns países europeus. Desde então, a necessidade de regulação da proteção de dados foi sendo discutida. Em 2011 o *European Data Protection Supervisor* (EDPS), publicou uma opinião nesse mesmo sentido. Ao longo dos anos muitos debates foram existindo, culminando com o regulamento 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016, dando então origem ao regulamento geral sobre a proteção de dados (RGPD). A sua transposição para a ordem jurídica nacional chegou em 8 de agosto de 2019 com a Lei nacional de execução 58/2019 que visa assegurar o seu cumprimento.

O avanço tecnológico, a globalização e no fundo toda a nova era digital que marca o século XXI, permitem que a informação circule em tempo real. Com a criação do mercado digital único, e de acordo com uma estratégia de proteção para assegurar os direitos e liberdades individuais no que diz respeito à privacidade dos dados pessoais surge este regulamento.

O interesse pela temática surgiu através de um seminário temático realizado no âmbito do mestrado em auditoria. Deste modo, a ideia era descobrir e investigar mais sobre o tema podendo aprender coisas novas sobre esta temática tão atual.

A presente dissertação está dividida em três capítulos. No primeiro capítulo procede-se à revisão da literatura, no segundo apresenta-se a metodologia utilizada, e no final é analisado o estudo do caso ímpirico seguido das respetivas conclusões.

No primeiro capítulo será feita a exposição dos conceitos teóricos sobre o tema, e nesta fase incial é pretendido perceber as particularidades do regime e todos os conceitos a ele associados. Este primeiro capítulo divide-se em cinco grandes subtemas, iniciando-se pelo enquadramento do RGPD no seu âmbito de aplicação e objetivos, seguindo-se o desenvolvimento da temática de dados pessoais e tratamento, passando de seguida pelas obrigações e, responsabilidades e no final da revisão da literatura, apresentam-se as questões de investigação elaboradas.

No segundo capitulo é descrita a metodologia utilizada para recolha de dados que sustentam a presente dissertação, é explicado o modelo de análise e relacionadas as questões com as hipóteses de investigação. Os dados serão recolhidos através de questionário e pedido de comentário de acordo com as hipóteses em estudo. A caracterização da amostra recolhida é ainda realizada neste capítulo.

No último capítulo serão apresentados os dados recolhidos e interpretados os resultados obtidos de acordo com a abordagem quantitativa e qualitativa.

Por último, destacam-se as conclusões decorrentes da investigação. Também as limitações encontradas durante a realização do estudo, assim como, sugestões para investigações futuras serão apresentadas no final da conclusão.

1 Enquadramento de conceitos

Para Coutinho (2011, p.55), "um dos primeiros propósitos de uma investigação é gerar informação que possa contribuir para uma melhor compreensão do fenómeno social em estudo". Este defende ainda que uma boa revisão da literatura pode dar maior credibilidade á investigação em causa, uma vez que, relaciona o problema que se pretende dar resposta com o conhecimento existente.

A revisão da literatura é para Prodanov e Freitas (2013), "o momento em que se situa o trabalho", trata-se de uma fundamental contextualização tanto para o leitor como para o autor, e para ambos os autores é também a fase que se respondem às questões "quem já escreveu e o que já foi publicado sobre o assunto".

É percetível o peso e relevância deste primeiro capítulo na investigação, e antes do desenvolvimento da mesma é pretendida então a explicação de vários conceitos necessários para melhor compreensão do estudo a realizar, com base em bibliografia consultada sobre o tema.

1.1 Proteção de dados na União Europeia e surgimento do RGPD

De acordo com Vieira (2007), questões ligadas à violação de dados pessoais estão diretamente relacionadas com os países mais desenvolvidos ao nível do tratamento automatizado de dados, ou seja, mais avançados tecnologicamente. Deste modo países membros da união europeia e os EUA destacaram-se nas primeiras ações sobre proteção de dados.

A temática sobre as informações armazenadas em bases de dados e a sua proteção terá surgido em meados do século XX, a importância pela privacidade começou a adquirir maior ênfase no panorama do direito europeu e internacional.

Foi no ano de 1950 que o conselho da europa (CdE), adotou a convenção europeia dos direitos do homem (CEDH), e nesta ficou expresso que "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". [1]

[1] Artigo 8º, Convenção europeia dos direitos do homem

Foi sendo desenvolvida legislação[2] de modo a dar solução ao problema, embora estas tentativas viessem a mostrar-se ineficazes. Nesta fase inicial partia-se ainda do princípio que apenas "poucos e gigantescos centros computacionais controlavam os dados; portanto, a ofensa necessariamente partiria dessas grandes empresas". (Vieira, 2007, p.232) A atitude tomada pelos governos passava pela atribuição de autorização a essas entidades para tratarem da privacidade. A total falta de controlo veio a concretizar-se uma certeza, tanto pelo governo como pelas próprias entidades.

O tratado de Roma (1957), trouxe o nascimento de uma organização: a comunidade económica europeia (CEE) que estabeleceu um mercado comum europeu, e desta forma, legislação comum em matéria de tratamento de dados era mais do que nunca necessária.

Apesar de ainda muito vagamente este tema foi abordado em Portugal na nova constituição de 1976, que estabelecia o direito dos cidadãos ao conhecimento de registos mecanográficos pessoais, as finalidades de registo, tendo poderes de exigir a sua retificação e atualização.

Decorria o ano de 1981, quando foi aprovada a convenção nº 108 pelo CdE, um marco importante pois estabeleceu várias medidas ao nível da proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Segundo Saldanha (2019, p.11), esta convenção surge devido "à necessidade de adequar a proteção dos direitos individuais a estas novas realidades" de acordo com o avanço nas tecnologias de informação.

Apesar dos esforços desenvolvidos, permanecia a diversidade jurídica dos estados membros, permaneciam as dúvidas quanto às adaptações necessárias e necessidade de harmonização. É só no ano de 1995 que é aprovada a diretiva 95/46/CE, do parlamento europeu e do conselho relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dos mesmos para harmonizar todas a distintas legislações existentes nos estados membros.

[2] 1973 Data Protection Act; 1974 Privacy act; 1978 várias medidas adotadas por França e Alemanha

Com a aprovação da diretiva europeia que estabeleceu que os estados membros tem de assegurar "a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais", começamos a assistir a uma mudança de mentalidades e a uma consciencialização cada vez maior para a proteção de dados. Esta diretiva tornou-se então uma referência para os estados membros e sendo uma diretiva europeia é vinculativa impulsionando à criação de legislação nacional. Em Portugal a resposta surgiu através da criação da Lei 67/98 de 26 de outubro (Lei da Proteção de dados).

O artigo 8º da Carta dos direitos fundamentais da União Europeia, estabelece em 2000:

"Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito"

A proteção de dados torna-se um direito fundamental, quando entra em vigor em 2009 o Tratado de Lisboa, assinado em 2007 [3]. Existe neste momento base jurídica específica e uma concordância com o estabelecido pela Carta dos direitos fundamentais da UE.

Vários regulamentos foram sendo desenvolvidos nesta matéria, e em 2011 a autoridade europeia para a proteção de dados (AEPD) emite um parecer definindo a necessidade de legislação para a proteção de dados e sugestões de melhoria. Incentiva a comissão europeia a ser pró-ativa em novos regulamentos, a busca de cooperação e o controlo de conformidade.

Novos pareceres e propostas vãos sendo desenvolvidos, e em 2014 o parlamento europeu demonstra o seu apoio esmagador na votação em plenário. Em 2015 entre uma abordagem geral sobre o RGPD pelo CE e recomendações da AEPD sobre o texto final do RGPD, O CE, PE e Comissão chegam a acordo.

É definido o plano de ação para a implementação do RGPD, em 26 de abril de 2016 é aprovado pelo parlamento europeu e do conselho o Regulamento Geral de proteção de dados (Regulamento UE 2016/679), entrando em vigor 20 dias após a publicação no jornal oficial da UE.

[3] Este tratado aproximou conselho europeu (define as orientações e prioridades políticas gerais da União Europeia) e parlamento europeu (poder legislativo, orçamental e de supervisão) conferindo-lhes a mesma competência.

O Regulamento geral de proteção de dados (RGPD) *ou General data protection regulation (GDPR)* é então um diploma (2016/679) do parlamento europeu e do conselho de 27 de abril de 2016.

Este novo regime veio revolucionar toda a forma de proteção de pessoas singulares face ao tratamento dos seus dados pessoais e a livre circulação dos mesmos.

Com o elevado avanço tecnológico e a globalização, cada vez mais se tornou fácil e rápido a partilha e armazenamento de informação. E toda esta evolução no tratamento automatizado de dados nos fez olhar para a proteção dos nossos dados pessoais de outra forma.

Tal como nos explicam Cunha, Hierro e Silva (2020), o progresso crescente ao nível da tecnologia e economia digital, apesar de nos marcarem por desenvolvimentos benéficos que nos serviram a vários níveis, também nos trouxeram consequências, trazendo uma perda de controlo sobre a transmissão de dados pessoais. O desenvolvimento de um mercado único digital estabeleceu as bases para que não existissem barreiras entre a livre circulação de mercadorias, pessoas, serviços e capitais, entre os estados membros da UE. E neste sentido e face a estas mudanças o nível de proteção tem de ser assegurado, a resposta para este problema surge com o Regulamento geral de proteção de dados.

1.1.1 Legislação aplicável em Portugal

A partir de 27 de abril de 2016 houve um período de adaptação dos estados membros ao regime e este tornou-se aplicável desde 25 de maio de 2018, vindo este regime revogar a diretiva 95/46/CE que se encontrava transposta em Portugal através da Lei da Proteção de dados (Lei 67/98 de 26 de outubro).

Em Portugal havia necessidade de legislação dado o cenário caótico que existia relativamente a esta matéria. Foi então criada a lei de execução Lei 58/2019 de 9 de agosto, trazendo algumas especificidades e que funciona como complemento da legislação europeia. Temos ainda em Portugal legislação de âmbito mais específico, na área de redes e serviços de comunicações eletrónicas acessíveis ao público: a Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto.

Em Portugal a entidade competente para fiscalização e controlo do tratamento de dados pessoais face às disposições legais é a CNPD (Comissão nacional de proteção de dados).

Também faz parte da alçada da CNPD proceder a avaliações, autorizações e pareceres em casos específicos. Esta atua junto da assembleia da república a nível nacional, mas também coopera com autoridades de outros estados para proteção de direitos de pessoas residentes no estrangeiro.

1.1.2 Âmbito de aplicação

O RGPD é claro nos seus artigos 2ºe 3º quanto ao âmbito de aplicação territorial e material, e é a partir daqui que vamos tentar perceber se a organização recai no âmbito de aplicação do RGPD.

Este regime abrange qualquer pessoa singular ou coletiva, pública ou privada que trate de dados **pessoais**, sendo importante destacar que não são abrangidos dados de pessoas **coletivas.**

O tratamento dos dados é indiferente, em todos os casos, estão abrangidos pelo RGPD, sejam eles total ou parcialmente automatizados. Bem como, dados pessoais contidos em ficheiros ou destinados a constar nestes [4].

A empresa subcontratante que trata dos dados pessoais por conta do responsável pelo tratamento dos mesmos é também alvo de aplicação do RGPD.

E temos ainda de esclarecer que, independentemente de o tratamento dos dados ocorrer dentro ou fora da UE, desde que o estabelecimento do responsável pelo tratamento ou do subcontratante se encontre na UE estará também sujeito ao regulamento.

Segundo Magalhães e Pereira (2018), são os três requisitos descritos anteriormente que nos fazem perceber a obrigatoriedade de cumprimento do RGPD numa entidade:

a) Organismo procede ao tratamento de dados pessoais
b) Organismo em causa é responsável pelo tratamento
c) Existe ligação geográfica do estabelecimento com a UE

[4] Como explicam Magalhães e Pereira (2018), estes ficheiros referem-se a um conjunto estruturado de dados acessíveis com determinados critérios pré-estabelecidos.

1.1.3 Objetivos do RGPD

Este regulamento além do objetivo primordial de servir de reforço à proteção de dados respondendo á carta dos direitos fundamentais da EU:

- ⇨ Assentou como um dos pilares base do EU Digital Single Market (mercado único europeu que abrange o marketing digital, eletrónico e as telecomunicações);
- ⇨ Harmonizou toda a legislação existente sobre proteção e tratamento de dados pessoais, trazendo a necessidade de criação ou atualização da mesma nos estados membros;
- ⇨ Fortalecimento da privacidade os titulares dos dados pessoais que se encontram na EU, passam a ter mais controlo sobre os mesmos (sabem onde estão e como querem que sejam tratados);
- ⇨ Trouxe a necessidade de restruturação e adaptação de como as organizações passam a abordar a privacidade dos dados pessoais;

1.2 Dados pessoais e tratamento

Entendemos por dados pessoais todas as informações relativas a uma pessoa singular viva identificada ou identificável, quer sejam dados relacionados com a vida pessoal, profissional ou pública. Incluem-se também todos os conjuntos de dados distintos que permitem a identificação de uma pessoa.

Estão incluídos também na categoria de "dados pessoais" todos aqueles que tenham sido de alguma forma codificados, descaracterizados ou pseudonimizados e que ainda assim permitem a identificação de uma pessoa. Os dados tornados anónimos, só o são assim considerados e excluídos do âmbito de dados pessoais se o processo de anonimato for irreversível.

Podemos então tomar como exemplos de dados pessoais os seguintes:

1. nomes, moradas, e-mail, idade, estado civil, situação patrimonial
2. Imagens de pessoais recolhidas em câmaras de videovigilância, assim como todas as informações pessoais obtidas no domínio das telecomunicações (gravação de chamadas, dados de tráfego, localizações, endereços IP).
3. E ainda, dados de caráter especial de tratamento apenas autorizado em casos excecionais, dos quais, vou escrever em detalhe de seguida.

Sempre que existam dúvidas quanto à natureza dos dados deve ser consultada a autoridade de controlo para os devidos esclarecimentos.

1.2.1 Categorias especiais de dados: Dados sensíveis

São apresentados como categorias especiais de dados que merecem relevância de tratamento devido à sua natureza, e por isso carecem de atenção especial. São dados que podem interferir com direitos e liberdades fundamentais de acordo com o contexto que são tratados e por regra é proibido o tratamento desses mesmos dados exceto quando previsto por disposição legal.

São exemplos destes dados, todos os que são referentes a:

- ⇨ Convicções filosóficas ou políticas
- ⇨ Filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica
- ⇨ Á saúde e à vida/orientação sexual, incluindo os dados genéticos
- ⇨ Dados biométricos que permitam a identificação da pessoa

Regra geral é proibido efetuar tratamento dos dados genéticos, biométricos, relativos a saúde e vida/orientação sexual. Mas, no entanto, podem existir exceções, tais como, quando existe consentimento explicito, necessidade para matérias laborais, judiciais, interesse público, saúde pública, medicina no trabalho.

Ainda existe legitimidade de tratamento quando, o titular tenha manifestado explicitamente e publicamente esses dados.

Por todas a razões apresentadas de complexidade de tratamento, estes estão sujeitos a condições de tratamento específicas.

1.2.2 Formas de tratamento de dados pessoais

- ⇨ Recolha
- ⇨ Retificação
- ⇨ Registo
- ⇨ Alteração
- ⇨ Recuperação
- ⇨ Conservação

- ⇨ Divulgação
- ⇨ Consulta Adaptação
- ⇨ Utilização
- ⇨ Organização
- ⇨ Destruição
- ⇨ Comunicação por transmissão ou difusão
- ⇨ Comparação
- ⇨ Apagamento
- ⇨ Limitação

Todas estas operações são exemplos que dizem respeito a formas de tratamento de dados pessoais e que podem ser realizadas com ou sem recursos automatizados.

De entre os exemplos de dados pessoais que podem ser tratados ao nível de estrutura empresarial temos:

- ⇨ Dados de recrutamento
- ⇨ Dados do pessoal
- ⇨ Dados de clientes
- ⇨ Dados de parceiros (fornecedores/prestadores de serviços)
- ⇨ Dados pessoais de utilizadores de websites

O que ter em conta antes de iniciarmos o tratamento dos dados?

- ⇨ Tratam-se ou não de dados sensíveis?

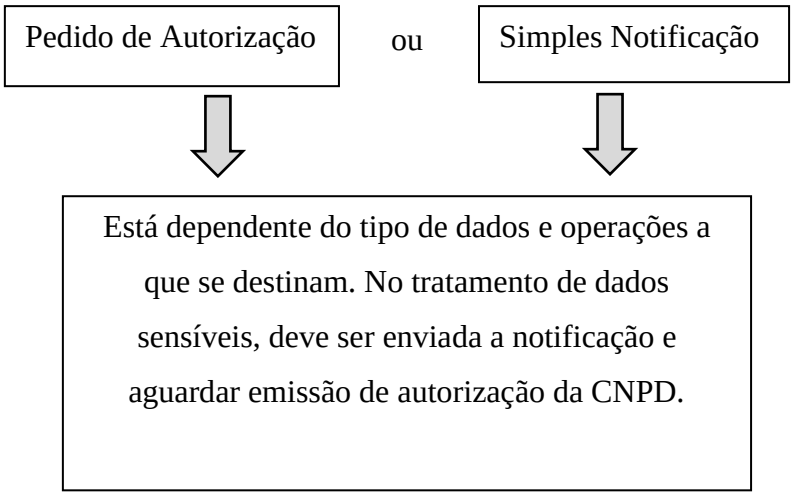
Figura 1 - Dados sensíveis

Fonte: APDSI (2014)

Como já exposto, o primeiro passo de tratamento será perceber se os dados são sensíveis ou não, pois por regra é proibido o tratamento dos mesmos, salvo algumas exceções.

O processo de tratamento deverá sempre ser iniciado pelo pedido um consentimento ao titular dos dades (pessoa a quem os dados dizem respeito). O segundo passo será notificação ou autorização à CNPD, consoante os casos: passo importante para qualquer empresa que se se torna responsável pelo tratamento de dados pessoais.

Figura 2 - Autorização/Notificação CNPD



Fonte: Elaboração própria (2020)

1.2.3 Princípios gerais subjacentes ao tratamento de dados pessoais

Em primeiro lugar o tratamento dos dados deve ser lícito (**Licitude**).

Licitude no tratamento dos dados

O tratamento dos dados torna-se lícito se cumprir de um dos seguintes requisitos:

- ⇨ Há consentimento da parte do titular dos dados
- ⇨ Execução de diligências pré-contratuais ou do próprio contrato
- ⇨ Cumprimento de uma obrigação jurídica
- ⇨ Este tratamento seja em virtude da defesa dos direitos e interesses vitais do titular dos dados

- ⇨ Exercido por uma autoridade pública ou no exercício de funções de interesse público
- ⇨ Sempre que necessário desde que os interesses do responsável sejam legítimos, desde que não prevaleçam os interesses do titular.

Deve também ter um objeto de tratamento leal (**lealdade**), e transparente (**transparência**), em relação ao titular dos dados.

As finalidades de recolha devem ser explícitas, determinadas e legitimas, e muito bem definidas, levando-nos ao princípio de **Limitação das finalidades.**

Os dados devem ser adequados e pertinentes: **Minimização dos dados.**

Todos os dados devem ser exatos (**exatidão**), e atualizados, sempre que não cumpram estes princípios devem ser eliminados ou retificados.

Devem ser conservados só durante o período necessário, embora possa ser prolongado este período sempre que de arquivo de interesse público: **Limitação da conservação**.

A segurança contraintenções de acesso ilícitas deve ser precavida assegurando a **Integridade** e **confidencialidade** dos dados.

1.2.4 Direitos dos titulares dos dados

Sendo as principais partes interessadas no meio de tudo isto, os titulares dos dados têm salvaguardados um conjunto de direitos pelo responsável pelo tratamento de dados.

Têm direito ao acesso (saber exatamente quais os seus dados que estão a ser tratados, por quem e como, assim como, ser-lhes garantido o acesso). O direito de retificação (sempre que os mesmos estejam desatualizados, incorretos ou incompletos). O direito de apagamento, esta é uma das grandes mudanças com o novo regulamento, apesar de existirem limitações. O titular pode fazer-se valer deste direito desde que os dados em questão se revelem desnecessários, queira retirar o consentimento, se oponha que os seus dados sejam tratados para fins automatizados e/ou de *profiling*. Este direito já não prevalece, sempre que, os dados tenham de se manter conservados por razões de interesse publico, segurança nacional faturação, fundamentos legais, ficais, entre outros com necessidade especifica. Está previsto também o direito á limitação de tratamento, este

direito prende-se com princípios explicados anteriormente, a exatidão, a licitude e as limitações.

Uma outra novidade introduzida pelo RGPD é o direito de portabilidade dos dados, que se relaciona diretamente com o direito de acesso. Difere deste último, pois o objetivo do direito à portabilidade dos dados, é em todo o momento poder obter os seus dados e poder dar-lhes novo uso (podem ser copiados, transferidos ou transmitidos mais facilmente por meios informatizados). Visa promover também a partilha segura dos dados.

O titular, beneficia também do direito de oposição e decisões individuais automatizadas, quer isto dizer que, o titular se pode opor ao tratamento dos seus dados pessoais, desde que apresente a devida justificação. Por sua vez o responsável pelo tratamento deve atender ao pedido e cessar o tratamento, salvo justificação incontestável, para efeitos previstos e justificados, nomeadamente questões de processos judiciais.

Por último, mas não menos importante, temos o direito, mas também o dever à informação. E neste em particular falamos em direito e dever, por existir dever específico pelo responsável pelo tratamento de fornecer ao titular o conjunto de informação sobre os dados recolhidos.

1.2.5 Consentimento

O consentimento é um dos pilares do RGPD. Este defende que o titular dos dados tem de dar o seu consentimento livre de espontânea vontade para os seus dados serem tratados em determinada finalidade claramente definida à priori. Além de livre o consentimento tem de ser informado especificamente, explicito e de forma a não haver lugar a equívocos. A revogação do consentimento deve ser simples, tanto quanto a sua conceção.

1.2.6 Tratamento dados pessoais – contexto laboral

A relação laboral envolve necessariamente recolha e tratamento de dados pessoais, como consequência do contrato de trabalho, para o tratamento de dados neste contexto o RGPD estabelece que se trata de uma situação especifica de tratamento.

Neste contexto, surgem vários exemplos decorrentes desta mesma relação, em que é necessário o tratamento: recrutamento, recibos de vencimento, baixas médicas, formação

profissional, celebração ou cessação de contratos, planeamento e gestão do trabalho, saúde e segurança no trabalho, entre outros. E neste contexto o regime é aplicado a:

- ⇨ Trabalhadores (nacionais e estrangeiros)
- ⇨ Estagiários
- ⇨ Subcontratados
- ⇨ Bolseiros
- ⇨ Pessoas coletivas e empresários em nome individual

Existem direitos e deveres a cumprir em ambas a partes, trabalhador e entidade empregadora, embora o trabalhador seja a parte mais fraca desta relação dado estar sob supervisão e autoridade superior. No código do trabalho encontra-se prevista a proteção dos dados pessoais nomeadamente à vida privada, no entanto o RGPD trouxe proteção mais detalhada e específica ao trabalhador nas várias "regras" a seguir no tratamento dos seus dados pessoais.

Se por um lado, o trabalhador passa a estar mais protegido, o empregador, terá de definir vários controlos de modo a garantir a que cumpre todos os requisitos garantindo também a sua própria segurança de acordo com a legalidade.

Saldanha (2019), sugere um conjunto de controlos a rever para melhor monitorizar a segurança do trabalhador, serão destacados os mais importantes. O ponto de partida será verificar se o contrato de trabalho celebrado contem alguma norma que determine a proteção de dados pessoais dos trabalhadores, caso não existisse verificar se foi feito algum aditamento. E logo de seguida verificar se existe lugar ao tratamento de dados pessoais do trabalhador, e se são só os estritamente necessários de acordo com as finalidades, de forma transparente. Deve ser feita também a verificação se existe limitações no acesso a esses dados, e verificar se os dados são alvo de armazenamento, transferência, fornecimento a terceiros.

Entidades subcontratadas

As entidades quando têm acesso a um conjunto de dados pessoais decorrentes de terem sido contratadas para prestação de algum serviço (exemplo das entidades subcontratadas),

passam a ter responsabilidades acrescidas. Neste caso, são também alvo de aplicação do RGPD, pois desenvolvem operações de tratamento de dados pessoais.

1.3 Obrigações e responsabilidades

Uma qualquer organização tem obrigações e responsabilidades para cumprir o regime geral de proteção de dados, que é então em alguns casos, obrigatório. Como já vimos, qualquer empresa que trate dados individuais ou agregados se torna responsável por eles e deve ter em consideração a forma como os trata devendo salvaguardar-se assegurando alguns aspetos.

Um dos aspetos mais importantes no tratamento prende-se com as finalidades para os quais são recolhidos: estas devem ser determinadas, explícitas e legítimas, para que não sejam usados com outros fins para os quais não eram destinados.

Os dados recolhidos devem ser só os pertinentes, nada além do estritamente necessário face ao objetivo de recolha dos mesmos, estes devem ser exatos e atualizados (devendo ser só mantidos também durante período necessário).

E é neste sentido que Magalhães e Pereira (2018), defendem que as empresas devem reger-se pelo princípio da *accountability*, que se traduz na garantia por parte das organizações que não haverá lugar à fuga de informação ou tratamento ilegítimo, e conseguindo provar a todo e qualquer momento por meio de evidência que o regulamento é cumprido. Guiar-se por este princípio implica não só fazer prova de cumprimento, como adicionalmente desenvolver e implementar políticas de "data governance", de acordo com as mesmas autoras. É ainda aconselhada a implementação de mecanismos de verificação de conformidade, e a realização de auditorias de controlo continuo da eficácia das medidas implementadas.

O regulamento 2016/679 fornece-nos algumas linhas mestre que nos ajudam a perceber como conduzir o tratamento dos dados. O artigo 25º sugere então a proteção de dados desde a conceção e por defeito, o artigo 330º o registo das atividades de tratamento, segurança na proteção de dados vem descrita no artigo 32º e obrigatoriedade de notificação explicita o artigo 33º.

É defendida a privacidade desde a conceção, ou seja, aquando a conceção de qualquer nova funcionalidade, programa, processo, novo produto seja tida em conta a proteção dos

dados desde o início. Na abordagem da privacidade por defeito, falamos de quantidade, disponibilização/acesso e prazos de conservação.

De acordo com o princípio da *accountability*, é aconselhada então a documentação e registo de todas as atividades de tratamento, assim como, todas as precauções em matérias de segurança adequadas ao risco. Mediante a organização, existem medidas recomendadas em matéria de segurança, entre elas: pseudonimizaçao e cifragem dos dados pessoais; garantia de confidencialidade, integridade, disponibilidade e resiliência; processos de teste e avaliação regular do grau de eficácia dos procedimentos.

Todas as entidades públicas ou privadas têm o dever de prestar a sua colaboração à CNPD (artigo 8º Lei 58/2019). Em específico o artigo 33º do RGPD, obriga à notificação da violação dos dados. Sempre que o responsável pelo tratamento detete que houve lugar à violação dos dados, seja por acesso indevido, fuga, ciberataques, deve comunicar à CNPD. A comunicação deve ser feita no prazo de 72 horas, também deve ser comunicado ao titular dos dados sempre a violação representar um alto risco para os seus direitos e liberdades.

Existem muitos tipos de dados e existem então dados que podem despertar mais interesse o seu conhecimento ou até o seu desaparecimento do que outros. Assim sendo é então necessário acautelar qualquer ação ilícita que possa ser desenvolvida sobre estes, como por exemplos a destruição (que também pode ser acidental), perda, partilha, acesso não autorizado. Em qualquer organização é a pessoa responsável pelo tratamento dos dados que deve desenvolver medidas que garantam um nível de segurança adequado face ao risco que apresenta o tratamento, tendo em consideração custos inerentes.

De modo a ter relativa segurança de que os dados estão protegidos devemos então definir uma estratégia que passa por:

1. Identificação das fraquezas do sistema (de modo a ter perceção dos riscos)
2. Cálculo da probabilidade (mais provável a falha aquando a comunicação de dados e quando há recurso á subcontratação) e impacto de determinadas ameaças
3. Definição de medidas de segurança adequadas de acordo com a entidade em questão, face ao analisado anteriormente

As organizações têm o ónus de provar que cumprem o regulamento. Importa acautelar registos de prova de cumprimento do RGPD. Neste sentido, também é essencial que as organizações sejam capazes de detetar uma fuga em tempo útil (Violação sobre os dados ou data breach). A notificação à CNPD de todas as violações que podem acarretar riscos para o titular é obrigatória, e tem um prazo máximo de 72h.

1.3.1 Avaliação de impacto

"Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos" (Magalhães e Pereira, 2019)

Já conseguimos perceber até então que intenção de todas as precauções a tomar em matéria de segurança visam salvaguardar os direitos e liberdades de cada pessoa (no âmbito de proteção de dados e privacidade). E assim sempre que, o tratamento poder resultar num alto risco deve ser realizada uma avaliação de impacto. Antes de proceder a esta avaliação o responsável pelo tratamento consultar previamente (art. 36º RGPD) a autoridade de controlo e comunicar-lhe os elementos estabelecidos no nº3 do mesmo artigo.

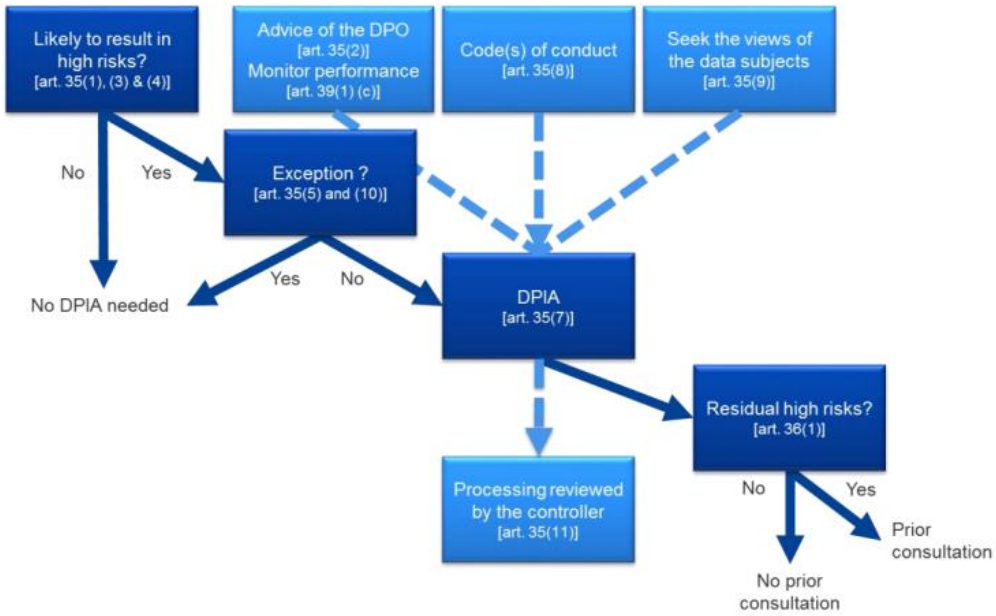
Estamos então perante de uma avaliação de impacto com base no risco. O EPD tem um papel fundamental nesta abordagem, uma vez que o que o RGPD exige que este tenha "em devida consideração os riscos associados às operações de tratamento, tendo em conta a sua natureza, o âmbito, o contexto e as finalidades de tratamento". Deve ser então dada prioridade às atividades de tratamento que estejam associadas a um maior risco, não desvalorizando também as de menor risco.

De acordo com a ISO 31000:2009, qualquer organização, independentemente da dimensão está sujeita ao efeito da incerteza sobre os objetivos, que nada mais é que um risco. De acordo com esta norma, após definição de risco, deve ser identificada a parte interessada, ou seja, quem pode ser afetada por algum acontecimento, que também pode ser chamado de stakeholder. As ações a tomar dizem respeito à gestão do potencial risco, ou sejas as medidas preventivas e de controlo, deve ser identificada a fonte do risco (elemento causador), probabilidade de ocorrência, e qual a consequência (resultado de

determinada ocorrência). Ainda deve ser acautelada, a eventual ocorrência de um evento que se traduz numa mudança de circunstâncias.

O esquema seguinte fornece-nos uma "ajuda" na perceção de quando deve ser realizada uma AIPD:

Figura 3 - Realização de uma AIPD



Fonte: Magalhães e Pereira (2018)

Uma AIPD pode ser utilizada para a avaliação de mais que uma operação de tratamento, desde que, se tenha em conta a natureza, âmbito, contexto finalidade e tipologia idêntica de risco. Dado que, este tipo de avaliação deve ser feita com regularidade, e tem sobretudo objetivo de a todo o momento detetar situações que possam ser suscetíveis de implicar risco para direitos e liberdades singulares, seja por mudança de circunstâncias ou novidades introduzidas é preferível que cada atividade deva ser analisada separadamente de acordo com o contexto específico associado.

O regulamento defende a elaboração e disponibilização para conhecimento público de uma lista ondem constem os tipos de operações de tratamento com elevando risco para a autoridade de controlo.

Em jeito de suma, e de acordo o regulamento e o grupo de trabalho 29, a metodologia a adotar numa avaliação de impacto cabe ao responsável pelo tratamento, no entanto deverá conter: Uma descrição sistemática das operações de tratamento previstas e a finalidade

de tratamento, avaliação da necessidade e relação de proporcionalidade ente as operações de tratamento com os objetivos, os riscos para as liberdades e direitos dos titulares, as medidas a tomar face aos riscos.

Podemos então concluir que a AIPD deve ser realizada antes de iniciar qualquer tratamento de dados, e de modo, a ajudar no posterior tratamento, priorizando atividades. É um processo continuo, pois, as organizações estão sempre em mutação, e além de todo o auxílio que presta ao desenvolvimento das tarefas do EPD e tomada de decisões tem o grande papel de **demonstrar conformidade**.

1.3.2 Implementação do RGPD

Para nos assegurarmos de que na nossa empresa este regime está a ser cumprido, devemos definir medidas e estratégias nesse mesmo sentido. Para isso deve ser traçado um plano de implementação do regulamento à medida das necessidades da empresa.

Para Magalhães e Pereira (2018), são quatro as grandes tarefas a desenvolver inicialmente. Em primeiro a designação de um responsável pelo compliance, posteriormente o levantamento e mapeamento de todos os tratamentos de dados pessoais, de seguida fazer um diagnóstico e por último as avaliar as medidas a tomar para garantir o compliance.

Grande parte das organizações está obrigada a nomear um responsável para a garantia do compliance nesta matéria, e nas que não está presente esta obrigatoriedade é aconselhável que seja nomeado um. Sendo este como dito, o primeiro passo no processo de implementação. Para podermos executar alguma ação de implementação, adaptação ou até de melhoria do existente é quase certo que teremos de avaliar a situação atual. E assim sendo, deverão ser identificados todos os tratamentos de dados existentes e registados. É aconselhável, que este registo seja feito de acordo com o tipo de dados, ou seja, a sua categoria, finalidade de tratamento, prazo de conservação e área geográfica. Deste modo será mais fácil fazer a avaliação do impacto de potenciais ameaças, tanto dentro da organização, como a subcontratantes ou terceiros a quem os dados são transmitidos. A fase do diagnóstico, passa por rever tudo o que recolhermos, identificar as falhas e os pontos positivos. Depois de tudo sumarizado, estamos aptos para sugerir melhorias, políticas, medidas corretivas ou até novos procedimentos.

O responsável pelo tratamento dos dados deve garantir que os titulares dos dados têm acesso a toda a informação necessária neste âmbito, certificando-se pela prestação da informação e disponibilizando-se para esclarecimento de qualquer dúvida. É importante relembrar que é necessário fazer prova do cumprimento do regulamento, e por isso mesmo, a documentação de todas as atividades relacionadas com tratamento é essencial para demonstração da compliance. Neste registo devem constar, formas de tratamento existentes, prova de informação a titulares, avaliações de impacto, procedimentos definidos e políticas neste âmbito. Por último, para assegurar a divulgação das disposições constantes nas políticas ou regulamentos internos. E esta posição, em consonância com a prova por evidência de cumprimento, mecanismos de verificação frequente, e a promoção de auditorias de controlo da eficácia das posições tomadas até então, constitui uma verdadeira política de *data governance*, regendo-se pelo princípio da *accountability*, defendido pelas autoras Magalhães e Pereira (2018).

1.3.3 Encarregado de proteção de dados

Neste contexto surge a figura do encarregado de proteção de dados, que em algumas entidades se torna obrigatório, sendo uma novidade introduzida pelo RGPD em Portugal.

Este não carece de certificação profissional para o efeito, exerce a sua função com autonomia técnica e é obrigatório:

- ⇨ Em entidades públicas (exceto tribunais)
- ⇨ Em entidades que tratem dados pessoais em grande escala com um controlo regular
- ⇨ Em entidades que tratem categoriais especiais de dados também em grande escala
- ⇨ Em entidades que tratem condenações penais e infrações

Sabendo o que são os "dados sensíveis", facilmente percebemos quais as entidades obrigadas à nomeação do EPD. Para entidades públicas também é percetível a obrigatoriedade, assim como, para dados pessoais relativos a condenações penais e infrações. Mas quando passamos, para "dados em grande escala" e o "controlo sistemático", a abordagem já se torna um pouco menos clara.

Quando ao que diz respeito a tratamento de dados em grande escala, o Grupo de trabalho do artigo 29 expõe alguns aspetos a ter em atenção para esta determinação, transcritos do artigo:

- ⇨ 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

O controlo regular e sistemático, apesar de também não estar apresentada nenhuma definição explicita no RGPD, entende o GT 29 que são necessárias uma ou mais características das apresentadas de seguida.

Para o controlo ser regular:

- ⇨ Contínuo ou que ocorre a intervalos específicos num determinado período
- ⇨ Recorrente ou repetido em horários estipulados
- ⇨ Constante ou periódico

E para ser considerado sistemático:

- ⇨ Que ocorre de acordo com um sistema
- ⇨ Predefinido, organizado ou metódico
- ⇨ Realizado no âmbito de um plano geral de recolha de dados
- ⇨ Efetuado no âmbito de uma estratégia

O Encarregado de proteção de dados deve desempenhar as suas funções com autonomia e independência, e de modo a garantir que isto é assegurado os artigos 38º e 39º do RGPD estabelecem alguns critérios a serem seguidos. O responsável pelo tratamento deve garantir que o encarregado está envolvido com todas as questões de proteção de dados e em tempo útil, no entanto não pode em momento algum dar instruções de como este deve desenvolver as suas funções ou auxiliar na tomada de decisões. O EPD, não pode ainda ser penalizado por desenvolver as suas funções reforçando isto a autonomia do mesmo. Diretamente relacionado com a independência, prende-se o facto de não poder haver

conflito de interesses nas atividades que desenvolve, sendo mais comum quando o EPD tem outras funções para além das relacionadas com a proteção de dados. Cabe á entidade estabelecer e identificar cargos que possam ser incompatíveis com este.

A designação do EPD em alguns casos é então obrigatória, tal como explicitado e como estabelece o nº 1 do art. 37º, mas quais são então os aspetos a ter em conta na nomeação deste?

O Encarregado de proteção de dados deve ser designado com base nas suas competências profissionais e conhecimentos para desenvolver funções nesta matéria. Deve ter conhecimento da legislação em vigor, das tecnologias de informação e segurança dos dados. É demonstrado então, que apesar de não haver lugar a formação especializada certificada nem rigorosa, o mesmo deve ter conhecimentos do direito e práticas de proteção de dados, de modo a garantir que a organização a qual presta o serviço cumpre todas as obrigações legais nesta matéria. É também importante o conhecimento da organização e a capacidade de conseguir promover uma cultura de proteção de dados.

Cunha et al (2020), defendem ainda que para além de todos os requisitos a nível profissional, pesam também as capacidades pessoais no que respeita à integridade e ética com que deve desempenhar as suas funções. Para estes autores, a figura do EPD deve ter uma enorme versatilidade, capacidade de pensar "fora da caixa" e até um pouco de criatividade do desenvolver da atividade.

Neste sentido, defende Antunes em 2018, Giovanni Butarelli no relatório "Towards a digital ethics" de 2018, um dos membros do EDPS Ethics Advisory Group: "Hoje, a ética e a proteção de dados estão interligados como nunca", havendo cada vez mais interligação entre eles".

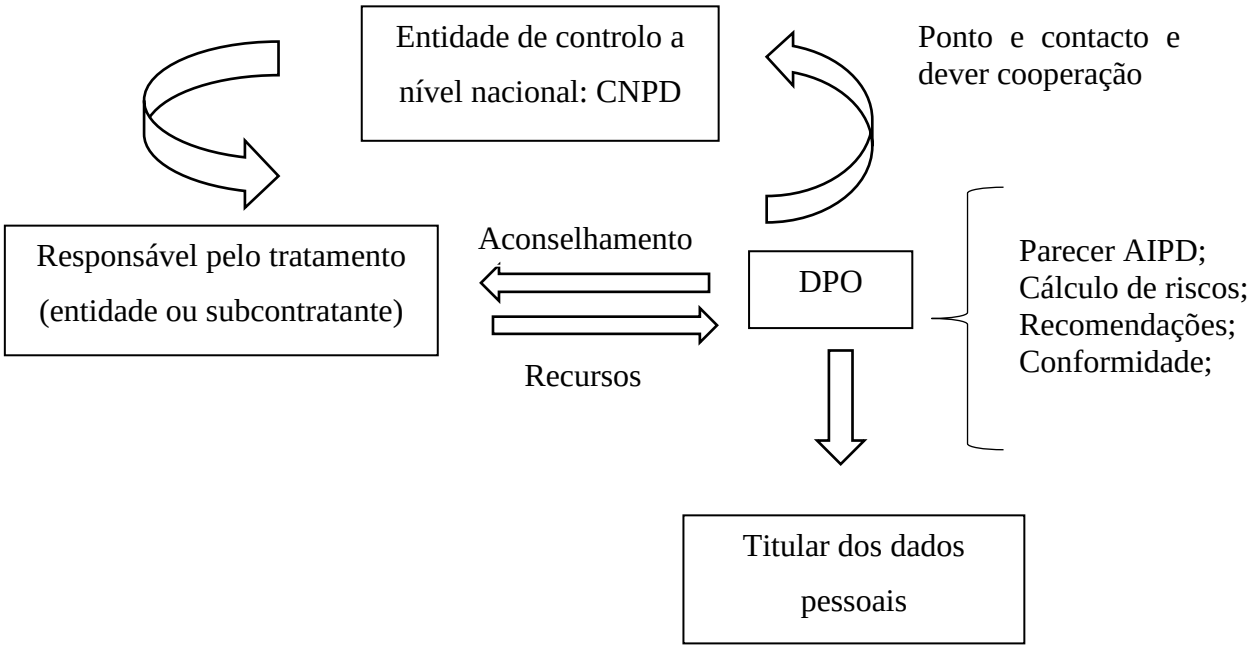
De acordo com o artigo 10º da Lei 58/2019 e o nº5 do artigo 38º do RGPD, este está obrigado ao dever de sigilo e confidencialidade em tudo o que diz respeito às suas funções.

Este tem, pelo menos, funções de informação e aconselhamento de todo o responsável por tratamento dos dados ou subcontratante. Ele controla a conformidades das práticas com o RGPD, e deve ser o ponto de contacto coma entidade de controlo e os titulares dos dados, cooperando com este. Deve ter em conta o risco associado às operações de tratamento e presta apoio à avaliação do impacto sobre a proteção de dados sempre que lhe for solicitado. Por sua vez, o responsável pelo tratamento, deve proporcionar todos os

recursos necessários ao desempenho do DPO, tais como, tempo suficiente para as suas atividades profissionais neste âmbito, apoio em termos de recursos financeiros, facilidades de acesso com todos os departamentos da organização para melhor comunicação e deve ser garantida também formação continua.

Conforme apresentado se seguida, as relações existentes entre os envolvidos em todo o processo de proteção dos dados, explicado anteriormente.

Figura 4 - Relações processo RGPD



Fonte: Elaboração Própria (2020)

1.3.4 Consequências de incumprimento

A autoridade de controlo promove a sensibilização e a compreensão do público alvo face ás regras existentes, riscos, direitos e garantias. Por outro lado, tem papel fiscalizador e de controlo, e assim sendo, podem surgir consequências negativas face ao incumprimento deste regime.

Do incumprimento de algumas disposições legais relativamente ao tema, podem advir responsabilidades criminais, civis ou contraordenacionais. Em conjunto a autoridade de controlo nesta matéria (CNPD) pode ainda aplicar sanções acessórias se assim o entender.

Toda e qualquer responsabilidade recai sobre o responsável pelo tratamento, pois este, de acordo com o nº1 do artigo 24º do RGPD, é quem "aplica as medidas técnicas e

organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado com conformidade" com o regulamento.

E para além de todas as consequências negativas acima referida, a imagem e reputação das empresas pode sempre ser posta em causa pelos stakeholders.

No caso de se traduzirem **contraordenações muito graves** (nº1 artigo 37 Lei 58/2019), as coimas a aplicar dividem-se por:

Grandes empresas: 5000€ a 20.000.000€, ou 4% do volume de negócios anual

PME: 2000€ a 2.000.000€, ou 4% do volume de negócios anual

Pessoas singulares: de 1000€ a 500.000€

No caso das contraordenações graves, os valores diminuem para metade em todos os casos.

No caso dos crimes a punição passa por pena de prisão na maior parte dos casos até 1 ano ou com pena de multa até 120 dias, são considerados crimes as seguintes ações:

- ⇨ Utilização de dados de forma incompatível com a finalidade da recolha
- ⇨ Acesso indevido
- ⇨ Desvio de dados
- ⇨ Viciação ou destruição de dados
- ⇨ Inserção de dados falsos
- ⇨ Violação do dever de sigilo
- ⇨ Desobediência

É ainda sempre punível toda a tentativa de cometer qualquer um destes crimes.

1.4 RGPD e a Auditoria

1.4.1 Auditorias de conformidade

Saldanha (2019), fornece etapas a realizar essenciais para a condução de uma auditoria de conformidade das entidades com o Regulamento geral de proteção de dados. As etapas defendidas pelo mesmo são as seguintes:

- ⇨ Recolha dos dados gerais da organização
- ⇨ Análise do tratamento efetuado aos dados
- ⇨ Verificação de cumprimento dos princípios do regulamento
- ⇨ Existência de cometimento dos titulares dos dados
- ⇨ Verificação dos requisitos de conservação dos dados

Olhando para estas etapas é percetível que se assemelham ás percorridas durante uma avaliação de impacto, e faz todo o sentido uma vez que AIPD visa sobretudo a demonstração de conformidade, e uma auditora externa também visa comprovar essa conformidade, mas do lado do "fiscalizador". E como em todas as auditorias, será emitido um parecer face ao trabalho efetuado.

Para que o processo de adequação com o RGPD seja efetuado da melhor forma, Cunha et al (2020) sugerem que este se divida em três fases: Fase 1, que se caracteriza por uma auditoria inicial com o diagnóstico e mapeamento dos dados, a fase 2 que se descrevem as medidas a tomar para a adequação e a Fase 3: a implementação das medidas necessárias para cumprimento. Durante estas três fases são muitos os trabalhos a desenvolver, no entanto é sempre aconselhado que todos os procedimentos e medidas recomendadas de demonstração do cumprimento com o RGPD sejam devidamente documentadas, assim como todos os processos que merecem mais atenção devem ser registados de modo a reportar tudo que será pertinente neste âmbito no relatório final.

Todas as informações recolhidas e analisadas nas três fases supracitadas serão agora relatadas em forma de um relatório final, que deverá conter todos os passos dados no decorrer da auditoria. A importância deste relatório prede-se não só com a finalidade principal de compliance com o RGPD, mas serve também de um suporte numa eventual fiscalização da CNPD. Como relembram Cunha et al (2020), não esquecer que este

relatório é de caráter confidencial, de uso exclusivo interno da entidade, não sendo aconselhável a partilha.

Foi então necessária a explicação deste processo de auditoria inicial para melhor percebermos a auditoria de conformidade que deve ser realizada posteriormente a esta abordagem inicial.

Segundo Cunha et al (2020), as auditorias de conformidade são realizadas a entidades enquadradas com o RGPD, na fase de fiscalização sucessiva ou depois da implementação das medidas nas entidades. São realizadas através de prestação de serviços e aconselhamento por parte do EPD e de uma equipa de auditores de dados competentes e designados para a condução desses trabalhos (estes trabalhos deverão traduzir-se numa acessória continua).

O papel do EPD, sendo responsável por controlar a conformidade com o regulamento (Art. 39º RGPD), é destacado nesta matéria, uma vez que este nos termos do artigo nº11 al. a) da LNE, deve assegurar a realização de auditorias quer sejam periódicas ou não programadas.

Conforme já dito, as auditorias de conformidade devem ser feitas de forma regular, no entanto não existe um nº definido de auditorias a realizar num determinado período. Cunha et al (2020), entendem que é necessário pelo menos uma auditoria anual, sendo que o número mais aconselhável pelos mesmos se fixa das duas ou três anuais. Devendo sempre ter em conta que esta regularidade também varia, de acordo com a dimensão da empresa, o nível de risco associado às atividades de tratamento, as categorias de dados tratadas, a avença do serviço contratado, entre outras.

A auditoria de conformidade pressupõe que já tenham sido efetuados esforços na busca pelo compliance com o RGPD e tomadas medidas, ou seja, que já tenha sido efetuada uma auditoria inicial de acordo com um processo de adequação ao RGPD.

E então, deve ser feita a avaliação da situação atual da entidade com atenção às medidas recomendadas, já implementadas ou não pela entidade, de modo a perceber se estão de acordo com o esperado, se serão necessárias alterações ou elaboração de novas recomendações.

Marques (2017), de acordo com a posição defendida em representação da CNPD na XXIV Conferência de Auditoria interna do IPAI, as auditorias competentes e

especializadas nesta matéria assumem particular importância. É defendida toda a colaboração na promoção à adoção de melhores práticas em matéria de RGPD e no cumprimento de todas as obrigações legais. De acordo com o mesmo, é importante todo o acompanhamento no desenvolvimento ou criação de sistemas tecnológicos e códigos de conduta. É destacado também o apoio no cumprimento de obrigação de realização das AIPD.

1.4.2 Auditoria interna

Num artigo de opinião publicado no site do IAPP, Haenebalcke (2018), defende que a necessidade de conformidade com o RGPD, levou a uma revisão dos planos anuais de auditoria interna.

Como já afirmado, o cálculo do risco antes do início do tratamento dos dados é essencial. Mesmo quando não é realizada uma avaliação de impacto, o risco tem de ser medido de qualquer das formas, de modo a perceber se estamos perante um risco elevado.

Para Haenebalcke (2018), a auditoria interna tem papel fundamental no apoio ao EPD auxiliando-o na conformidade com o RGPD. À partida, a auditoria interna é uma atividade de elevado valor para a organização. Esta atua fornecendo garantia independente de que os processos de gestão do risco e controlos internos são eficazes. E é neste mesmo sentido que a opinião de Haenebalcke segue, o auxílio da auditoria interna faz todo o sentido, uma vez que o objetivo de ambos é comum: minimizar o risco a que a organização está exposta.

Os profissionais de auditoria interna possuem experiência no que diz respeito a avaliações sobre a eficácia de medidas e controlos e emissão de pareceres e relatórios sobre estes. Com estas valências, em conjunto com a capacidade de desenvolver políticas e procedimentos de monotorização do risco, a auditoria interna torna-se um grande apoio no ponto de partida inicial para a implementação. Por sua vez, a auditoria interna, também beneficia com os conhecimentos especializados do EPD, para melhor conduzir as suas análises. Quando AI e EPD se encontram em sintonia e cooperação podemos perceber uns aliados perfeitos no caminho para a conformidade com o RGPD.

A relação existente entre auditoria interna e o compliance com o RGPD é fortemente defendida então por vários profissionais ligados a ambas as áreas.

Marques (2018), demonstra o novo rumo e importância atribuída à auditoria interna aquando a entrada em vigor do novo regulamento geral de proteção de dados no contexto da autorregulação. É defendida a atenção especial por parte da AI aos sistemas de informação procedimentos e processos internos de modo a cumprirem as demandas do RGPD.

1.5 Perguntas/Questões de investigação

Após um estudo sobre o tema e da revisão de toda a literatura surgem as perguntas de investigação.

Para Prodanov e Freitas (2013) a finalidade da pesquisa científica assenta em descobrir respostas para as questões mediante um método científico, e esta investigação parte sempre de um problema.

São expostas de seguida as questões de investigação a que é pretendido dar resposta:

Tabela 1 - Questões de investigação

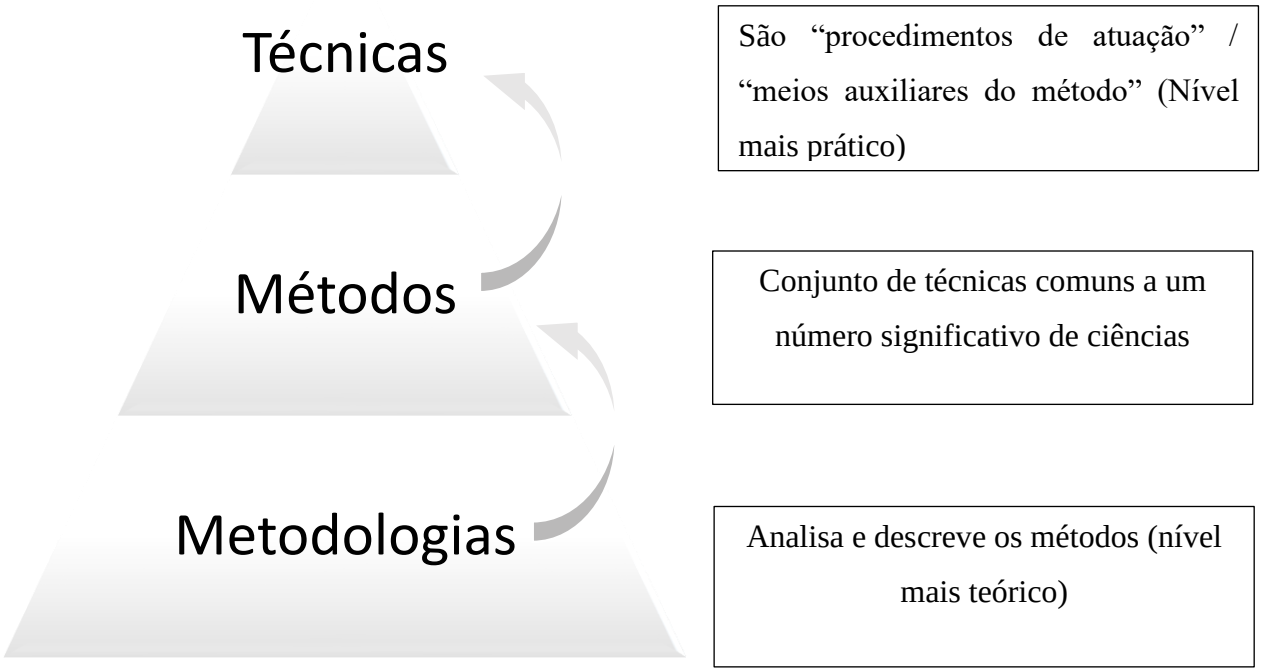
QUESTÕES	**AUTOR, DATA**
Questão 1: A obrigatoriedade de cumprimento do RGPD trouxe ás empresas grande impacto face á necessidade de adaptação?	Lambelho e Mendes, 2019 Antunes, 2018 Saldanha, 2019
Questão 2: Existe um elevado grau de resistência nas empresas para adoção do regime ou até foram percebidos benefícios?	Saldanha, 2019 Para Magalhães e Pereira, 2018
Questão 3: Existe conhecimento efetivo do regime?	Para Cordeiro, S. e Gouveia, L Para Magalhães e Pereira, 2018
Questão 4. Existe um encarregado de proteção de dados conhecido e este é devidamente qualificado para o cargo?	Regulamento 2016/679 Silva, 2018 Antunes, 2018
Questão 5: Existe contributo e utilidade da auditoria interna e da auditoria de conformidade (externa) para a compliance com o RGPD?	Para Saldanha, 2019 Para Hertzberg, 2018 IIA, 2019

2 Metodologias de investigação

Após o trabalho de revisão da literatura relevante sobre o tema a investigar, é necessário definir a metodologia que iremos adotar para tentar dar solução a todas as questões que foram surgindo durante a investigação feita no capítulo 1.

Para Coutinho (2011), há que distinguir metodologia, métodos e técnicas. A metodologia assume para ele um sentido mais abrangente, é influenciada pelas escolhas do investigador e abarca métodos e técnicas.

Figura 5 - Metodologia. métodos e técnicas



Fonte: Elaboração Própria (2020)

Sousa & Batista (2011) descrevem a metodologia de investigação como um "processo de seleção da estratégia de investigação, que condiciona, por si só, a escolha de técnicas de recolha de recolha de dados", e naturalmente que sejam as mais adequadas aos objetivos em estudo.

A metodologia para Prodanov e Freitas (2013), é uma disciplina que consiste em "estudar, compreender e avaliar os vários métodos".

Podemos compreender após coleta de opiniões dos vários autores que a metodologia de uma forma genérica se trata do caminho que nos vai levar à resolução da problemática

inicial, trata-se de um meio para a atingir uma determinada conclusão a partir de um estudo. E será esta a conclusão que podemos retirar através da origem etimológica da palavra "metodologia", composta por três vocábulos de origem grega "meta" ("para além de"), odòs ("caminho") e logos ("estudo").

2.1 Métodos de investigação

A definição do método a adotar assume um papel preponderante, pois será através deste que iremos conduzir a recolha dos dados para tratamento e análise.

Quanto aos métodos de investigação existentes, de forma genérica são classificados como método quantitativo, qualitativo e misto, apesar de as opiniões quantos aos mais capazes ou eficazes divergirem por vários autores.

Sousa M. e Batista C. (2011) defendem que o método quantitativo é caracterizado pelos padrões observáveis através dos dados identificados e apresentados a partir de uma amostra da população. De acordo com estes, o método apresenta como limitação o facto de não permitir ao investigador controlar as variáveis independentes.

Para Coutinho (2011), a teoria tem um papel crucial no desenvolvimento do método quantitativo e neste "o investigador deve levantar hipóteses e submete-las a confrontação empírica". Na opinião deste autor, o "paradigma positivista" como denomina o modelo quantitativo baseia-se em quantificação, generalização e previsão de fenómenos.

O método qualitativo surgiu, na opinião de vários autores como alternativa à abordagem positivista, face à incapacidade de resposta para todas as problemáticas do modelo quantitativo, como nos explica Coutinho (2011) e partilham da mesma opinião de Sousa M. e Batista C. (2011). É para eles um método que se centra na compreensão dos problemas, analisa comportamentos, atitudes, valores, o papel do investigador é fundamental neste tipo de abordagem. As vantagens deste modelo são estão destacadas pela eficácia no estudo da subjetividade, em oposição ao modelo anteriormente descrito. Os autores destacam ainda a vantagem de gerar boas hipóteses de investigação devido à análise de pormenores minuciosos durante entrevistas, relatórios, entre outros. O modelo apresenta a falha possível de falta de objetividade decorrente das capacidades ligadas ao investigador.

A combinação destes dois métodos também é bem vista por vários autores, que embora tratando-se de métodos diferenciados, podem complementar-se em algumas situações tornando a pesquisa mais rica, em termos de fiabilidade e validade.

2.1.1 Técnicas a adotar

As informações necessárias a recolher para tratamento serão então feitas na presente dissertação, através de questionários e uma forma de entrevista (foi pedido aos entrevistados que comentassem (dessem as suas opiniões pessoais sobre os assuntos em estudo).

É pretendida uma análise quantitativa realizada através de questionários, e complementar essa análise com uma abordagem qualitativa.

Como já referido anteriormente, a combinação dos dois métodos é vantajosa e bem vista por muitos autores, na medida que nos permite ter uma maior segurança dos resultados obtidos. Assim sendo, o método a utilizar será o método misto, para tentar não só perceber a frequência de determinada resposta ou opinião, mas também poder avaliar, interpretar, e compreender pormenores não percetíveis em questionário.

2.2 Hipóteses a analisar

De acordo com Punch (1998; citado por Coutinho, 2011, p.48), uma hipótese "é uma previsão de resposta para o problema de investigação".

A elaboração das questões que nos levam consequentemente às hipóteses, com base na revisão da literatura é essencial numa investigação. No desenvolvimento do estudo através de recolha de dados e análise de resultados obtidos é pretendido comprovar as hipóteses formuladas. Assim, ao testarmos as hipóteses, no fundo o que estamos a testar será a teoria que sustenta as mesmas, tal como defende Punch (1998).

Para Coutinho (2011), o exposto anteriormente faz sentido quando fazemos uma abordagem quantitativa. Para o mesmo autor a ausência de hipóteses "formalmente explicitadas" caracteriza a investigação não quantitativa, uma vez que o teor do problema não é ainda conhecido na fase inicial.

Para Sousa M. e Batista C. (2011) as hipóteses são afirmações acerca das relações entre as variáveis em estudo, por vezes baseadas em senso comum, não necessariamente verdadeiras, pois o objetivo será no final da investigação concluir sobre veracidade ou falsidade das mesmas de acordo com os "testes" realizados.

De acordo com Prodanov e Freitas (2013), o ponto de partida da investigação é a interrogação, como exposto anteriormente, e desse modo para solucionar o problema são levantadas hipóteses, confirmadas ou não pela pesquisa efetuada. Para este autor, toda a pesquisa se baseia nessa mesma "teoria" formulada. O autor esclarece ainda que estas hipóteses são afirmações e não interrogações, servem de guia condutor da investigação.

2.2.1 Perguntas de investigação e hipóteses

Lambelho e Mendes (2019) defendem que, para que os dados pessoais dos trabalhadores estejam protegidos e as empresas aptas para cumprir o regime é necessário um conhecimento elevado da legislação existente a este nível.

Para Antunes (2018), milhões de pessoas irão ver as suas vidas alteradas mediante decisões e mudanças de atitudes que o RGPD obrigada as entidades privadas a tomar.

Esta necessidade de compliance com o regulamento trouxe às empresas vários constrangimentos, tal como afirma Saldanha (2019) as relações laborais são prejudicas por excesso de zelo ou falta de conhecimento, assim como, aumentou as dificuldades de assinatura de contratos face ao consentimento exigido às empresas subcontratadas.

A necessidade de alguma adaptação por parte das empresas parece uma realidade, e esta pode ter sido maior ou menor face à sua capacidade e preparação. Todas estas teorias dos autores levam-nos a formular a primeira questão que procuramos dar resposta, apresentada de seguida.

<u>Questão 1:</u> A obrigatoriedade de cumprimento do RGPD trouxe ás empresas grande impacto face á necessidade de adaptação?

Na opinião de Saldanha (2019), é notória a desconfiança inicial na adoção do regulamento, no entanto, quando maior a preparação, mais este regime passa a ser visto

como uma oportunidade. Este defende que apesar da complexidade o regulamento foi bem recebido e relativamente bem compreendido.

De acordo com o mesmo autor a adoção de boas práticas de privacidade pelas organizações tem-se traduzido em melhores resultados, menos custos operacionais e clientes mais satisfeitos levando a uma melhor reputação e visibilidade do negócio.

Para Magalhães e Pereira (2018), as organizações "encaram este novo regulamento com alguma preocupação".

Por si só, todas as necessidades de mudança parecem trazem consigo algum receio face ao futuro.

Tal como nos explicam Magalhães e Pereira (2018) e exposto anteriormente, é necessário passar por várias fases para implementação do RGPD e em que é percebido um custo para estar em conformidade, seja devido a formação, tempo despendido, necessidade de contratação de novos profissionais, novos programas, entre outros, além de que existem sanções por não conformidade.

Dadas todas as necessárias mudanças pode surgir algum constrangimento por parte das empresas, e mesmo elevado grau de resistência. No entanto apesar dos problemas iniciais, é defendido que são percebidas mudanças positivas após implementação do regime. E é isto mesmo que é pretendido perceber com a seguinte questão.

<u>Questão 2:</u> Existe um elevado grau de resistência nas empresas para adoção do regime ou até foram percebidos benefícios?

Para Cordeiro, S. e Gouveia, L., o caminho para a conformidade com o regime é longo e tortuoso, em constante busca pela melhoria de processos e mudança de mentalidades até ao enraizamento de procedimento, não existem soluções imediatas. Para os mesmos autores, as empresas enfrentam mudanças culturais e informáticas, a forma como colaboradores agem deverá mudar, assim como, softwares informáticos que suportam as operações deverão ser redesenhados.

Para Magalhães e Pereira (2018), as obrigações e direitos que decorrem da aplicação do regime, quando se estava a menos de um ano da aplicação do mesmo eram ainda bastante desconhecidas. Isto leva-nos à terceira questão:

<u>Questão 3:</u> Existe conhecimento efetivo do regime?

Desta forma e após reflexão sobre as questões apresentadas e revisão da literatura surge a primeira hipótese de investigação.

Hipótese 1: As organizações conhecem o RGPD, mas este, trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas.

O regulamento 2016/679 criou um novo cargo nas empresas: o encarregado de proteção de dados e este deve ser designado sempre que, de acordo com a alínea c) do artigo 37º, as atividades principais do responsável pelo tratamento consistam em operações (…), que exijam um controlo regular e sistemático dos titulares dos dados em grande escala, entre outras em que a nomeação é também obrigatória (cfr. art. 12º e 13 da LNE e art. 37º do RGPD). O regulamento reconhece e destaca a vital importância do EPD para fazer face ao cumprimento das exigências do RGPD. Cunha et al. (2020), defendem que apesar de existirem casos em que a nomeação do EPD não é obrigatória, todas as entidades que procedem ao tratamento de dados pessoais devem fazer essa nomeação. Esta posição é defendida, na medida que, este será um dos primeiros passos para o compliance, funcionando como salvaguarda em futuras fiscalizações.

Silva (2018), destaca o encarregado de proteção de dados um dos intervenientes mais importantes neste novo panorama apresentado pelo RGPD.

Face ao conhecimento necessário e todas as obrigações a cumprir associadas ao regime, destacando a figura do encarregado de proteção de dados, que assume um papel de responsabilidade face ao cumprimento, levanta-se a seguinte questão e posteriormente é apresentada a segunda hipótese formulada:

<u>Questão 4.</u> Existe um encarregado de proteção de dados conhecido e este é devidamente qualificado para o cargo?

Hipótese 2: O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.

Para Saldanha (2019) uma auditoria de conformidade terá de dar confiança e comprovar que o regulamento está a ser cumprido. Também para este autor o processo de auditoria por si só, permite uma reavaliação de processos implementados. O que permite descobrir processos obsoletos ou informação armazenada desnecessária, o que se traduz numa mais valia no desenvolvimento da organização, podendo também passar a consumir menos recursos.

Para Hertzberg (2018), a auditoria interna pode ajudar a organização na fase de implementação do RGPD, permitindo calcular e mitigar os riscos e recomendar melhorias fortalecendo o controlo.

Como podemos perceber através de publicação no IIA (2019), a auditoria interna deve assumir a liderança, promovendo uma auditoria baseada no risco, avaliando a situação existente em matéria de governança do RGPD. A auditoria interna pode ajudar na gestão do risco e fornecer garantia significativa de conformidade.

Neste sentido é pertinente a seguinte questão e posterior hipótese de investigação nº3.

<u>Questão 5:</u> Existe contributo efetivo e utilidade da auditoria interna e da auditoria de conformidade para a compliance com o RGPD?

Hipótese 3: A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.

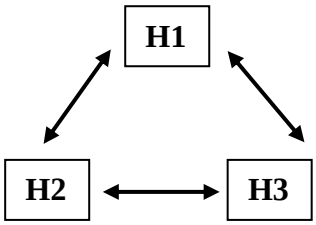
Tabela 2 - Hipóteses e questões de investigação

Hipóteses de análise	**Perguntas de investigação**
H1: As organizações conhecem o RGPD, mas este, trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas.	**Q1.** A obrigatoriedade de cumprimento do RGPD trouxe ás empresas grande impacto face á necessidade de adaptação?
	Q2. Existe um elevado grau de resistência nas empresas para adoção do regime ou até foram percebidos benefícios?
	Q3. Existe conhecimento efetivo do regime?
H2. O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.	**Q4**. Existe um encarregado de proteção de dados conhecido e este é devidamente qualificado para o cargo?
H3. A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.	**Q5.** Existe contributo efetivo e utilidade da auditoria interna e da auditoria de conformidade para a compliance com o RGPD?

Fonte: Elaboração própria (2020)

2.2.2 Modelo de análise

O modelo de análise pretende então explicar a forma como as hipóteses formuladas se interligam entre si.



A Hipótese 1 (As organizações conhecem o RGPD, mas este, trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas.), está diretamente relacionada com a hipótese 2 (O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.), uma vez que uma das grandes novidades do regime passa por, em algumas entidades a obrigatoriedade de designar um Encarregado de proteção de dados. E mesmo quando não obrigatório, deve haver um alguém que trate dessa tarefa. O Encarregado de proteção dados, obrigou as empresas a mudarem a sua forma de trabalhar, uma vez que, deve buscar continuamente de formação profissional, não havendo pessoa interna para ocupar o lugar deve recorrer-se a contratação externa. O RGPD, e em particular o Encarregado de proteção de dados, trouxe consigo várias mudanças, necessidades de adaptação e impacto para as organizações.

A Hipótese 2 (O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.), e a hipótese 3 (A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD), também se interligam entre si. A pessoa que desenvolve o cargo de encarregado de proteção de dados, tem de se preocupar a todo o momento com a gestão do risco, preocupação constante também no desenvolver dos trabalhos de auditoria (quer interna, quer externa). Cada uma á sua maneira (auditoria de conformidade e auditoria interna), devem prestar auxílio à empresa e em particular ao EPD que também deve recorrer a estas.

A hipótese 3 relaciona-se também inevitavelmente com a hipótese 1 acima mencionadas. Da preparação das organizações para a entrada do regime faz parte uma análise da situação existente em toda a organização em matéria de riscos para os dados pessoais tratados, tal como explicado anteriormente a auditoria inicial de adequação com o RGPD é um dos passos fundamentais no caminho para a compliance. A auditoria interna é (ou deve ser) também, parte integrante neste processo de implementação, estando associada a todos os processos de calculo de riscos e desenvolvimento e implementação de controlos na organização.

Percebemos então que as hipóteses se interligam entre si, não só porque todas ela contém elementos fundamentais no auxílio e apoio no compliance na organização (EPD, auditoria interna e de conformidade), como também este impacto e necessidade de adaptação recaiu sobre todas estas áreas.

2.3 Recolha de dados

A recolha de dados como explicitado anteriormente será feita através de questionário disponibilizados mais à frente (Apêndice I), assim como, pedido de comentário mais detalhado direcionado com as hipóteses de investigação.

O questionário é dividido em duas partes, a primeira sobre perfil do inquirido e a segunda sobre as perguntas pertinentes para tirar conclusões sobre as hipóteses formuladas. Os comentários sobre a temática apenas abordam temas pertinentes da temática em estudo. Em caso algum os envolvidos serão identificados, além do necessário.

Para o caso dos questionários, a identificação estreitasse apenas ao sexo, faixa etária e atividade profissional.

No que aos comentários diz respeito, será apenas referido o enquadramento profissional no individuo em questão.

A escala utilizada foi a escala de Likert. Esta escala consiste na elaboração de um conjunto de pequenas frases que traduzem um nível de concordância ou não com a questão em estudo. Normalmente esta escala é composta por cinco níveis que vão desde o “discordo totalmente” até o “concordo totalmente”. Na presente dissertação foram utilizados quatro níveis que correspondem às quatro opções de resposta (Discordo/Nem concordo nem discordo/Concordo em parte/Concordo totalmente). Esta escala foi

percebida como a mais pertinente, uma vez que nos permite avaliar a posição do inquirido face à questão em diferentes níveis, permitindo a este não só concordar totalmente ou discordar totalmente, como também não tem opinião ou concordar apenas em parte.

A plataforma de criação do formulário para questionário foi o Google Forms, e os cálculos auxiliares às conclusões finais foram trabalhados em Excel.

2.4 Definição da população e amostra

Uma amostra é um subconjunto de uma população, e ao número de elementos que fazem parte dessa amostra chamamos tamanho da amostra.

Para Prodanov e Freitas (2013) esta amostra deve selecionada de acordo com uma regra ou um plano e é esperado que seja representativa da população que se pretende estudar.

No presente estudo podemos definir a população como todos os profissionais ligados diretamente ao tratamento de dados pessoais na lista de empresas que integram o PSI 20.

Para a análise quantitativa foram então selecionadas as 18 empresas que atualmente compõe o índice das maiores empresas cotadas na Euronext Lisboa (PSI 20). Dentro de cada empresa, foi pedido que os inquéritos fossem disponibilizados ao encarregado de proteção de dados, área de auditoria interna e recursos humanos.

Esta seleção foi feita com base no critério, de quais seriam as empresas mais aptas em Portugal para conseguir responder as questões de investigação.

Para Saldanha (2019), "a boa utilização da privacidade acaba por ter um efeito económico positivo" e traz também benefícios para a reputação da organização, e para ele isto transforma-se não só em responder ao regulamento, mas também em potenciar os negócios (melhor reputação, consequente aumento da visibilidade da organização/produto/marca).

Sendo estas as "grandes" empresas portuguesas, são à partidas as mais preparadas em matérias de proteção de dados. É percebida a sua preocupação, nomeadamente nos sites com a privacidade. É disponibilizado, na maior parte dos casos, o email do encarregado de proteção de dados para eventuais esclarecimentos. Esta também foi uma das vantagens de escolha das empresas deste grupo.

Foi pedido ainda que os inquéritos fossem disponibilizados, dentro das empresas, nas áreas de recursos humanos e auditoria interna dado a forte ligação existentes entre estas áreas e a proteção de dados.

O questionário foi submetido em 26 de agosto de 2020 e posteriormente enviado pedido de resposta por email, o mesmo esteve disponível até 30 de setembro de 2020.

Para a análise qualitativa era pretendida uma opinião que seria confrontada com os resultados obtidos na análise quantitativa. Assim sendo, os profissionais escolhidos foram especialistas, com grande experiência e conhecimento de causa sobre a temática com quem tive contacto durante o percurso académico e na leitura da literatura pertinente neste âmbito.

2.5 Caracterização da amostra

2.5.1 Análise quantitativa

De acordo com uma abordagem quantitativa, aparenta-se o questionário elaborado para adequação e estudo das hipóteses de investigação.

Apresentamos de seguida o questionário elaborado para validação de cada uma das hipóteses em estudo:

Tabela 3 - Hipóteses e questionário

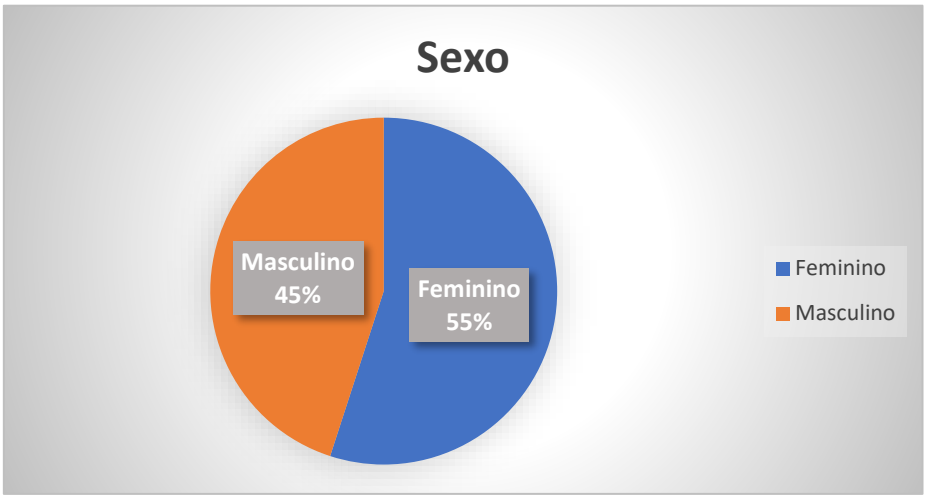
Hipóteses	Questões elaboradas (Questionário)
Hipótese 1	Tem conhecimento dos temas abordados pelo RGPD (Regulamento geral de proteção de dados?)
	Considero que a empresa se encontrava preparada quando o RGPD passou a ser obrigatório, proporcionando os recursos necessários e adotando medidas adequadas (Políticas, processos internos).
	Considero que o impacto do regulamento na empresa foi minimizado, dado que existiu uma consciencialização geral sobre a privacidade e proteção de dados dentro da organização.
	O tema tem sido "adiado" e não existe até então alterações significativas de processos, não sendo percebida muita preocupação e abertura para aplicação deste regulamento.

	Considero que este regulamento alterou substancialmente a forma de trabalho, trazendo várias preocupações, procedimentos adicionais e alterando vários processos existentes.
	A adoção de novas práticas á luz do RGPD trouxe melhores resultados ao nível de satisfação de clientes/funcionários/melhoramento de processos e menor utilização de recursos.
Hipótese 2	Tenho conhecimento que existe encarregado proteção de dados na empresa ou desempenho essa mesma função.
	Considero a temática bastante complexa, e sinto necessidade de formação profissional ou informação de esclarecimento sobre o tema.
	Considero que o encarregado de proteção de dados tem as competências profissionais necessárias e pertinentes para desempenhar as suas funções.
Hipótese 3	O trabalho realizado pelas auditorias de conformidade no âmbito do RGPD (externas) ajuda à clarificação de temas, fornece sugestões de melhoria e apoia na adoção de novos procedimentos.
	A auditoria interna tem um papel ativo no apoio ao cumprimento do RGPD, assumindo papel preponderante na gestão de riscos e definição de controlos.

Começado pela caracterização do inquirido, a preocupação com a não identificação da dos envolvidos foi uma constante. Apenas foi questionado o sexo, a faixa etária que se encontra inserido e de forma genérica a função ou departamento que ocupa à data de resposta. Dado que foram previamente definidos os destinatários dos questionários já eram previstos os cargos ocupados pelos inquiridos.

No seu total foram recebidas 20 respostas aos questionários. De acordo com o sexo foram obtidas 11 respostas do sexo feminino e 9 respostas do sexo masculino.

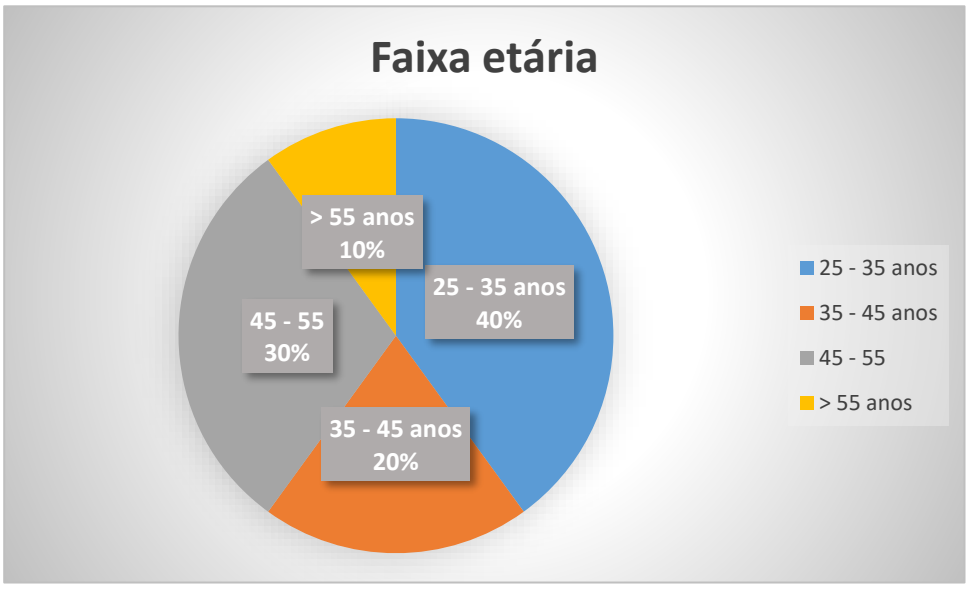
Figura 6 - Sexo dos inquiridos



Fonte: Elaboração própria (2020)

Quanto á faixa etária, a mais predominante situa-se entre os 25 e 35 anos, de acordo com o que traduz o seguinte gráfico.

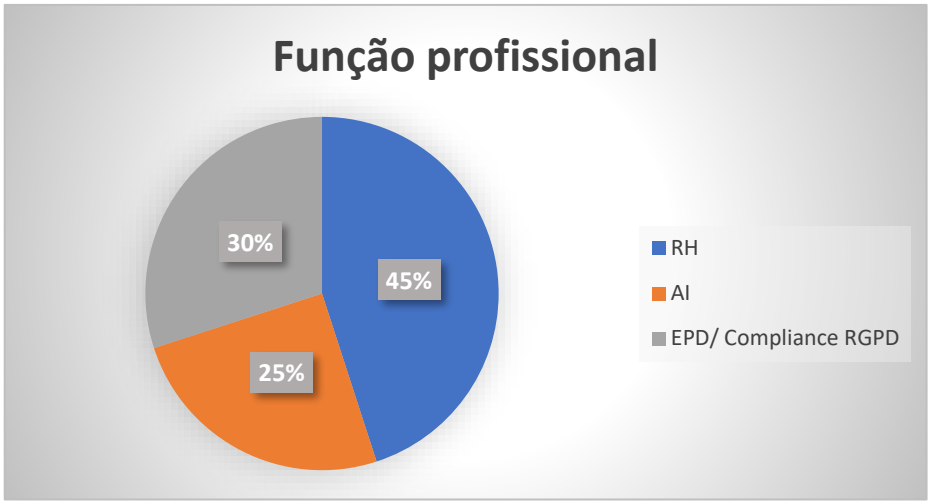
Figura 7 - Faixa etária dos inquiridos



Fonte: Elaboração própria (2020)

Foi pedido que o questionário fosse direcionado aos profissionais de recursos humanos, auditoria interna e encarregado de proteção de dados ou semelhante (pessoas responsáveis pela compliance com RGPD). E assim sendo, os resultados obtidos vão de encontro a isso mesmo. A amostra é então constituída por 9 profissionais da área de recursos humanos, 5 da área de auditoria interna e 6 na área de compliance com RGPD ou EPD.

Figura 8 - Cargo dos inquiridos



Fonte: Elaboração própria (2020)

2.5.2 Análise qualitativa

O método utilizado traduziu-se numa abordagem não tão habitual como a entrevista para esta análise. Normalmente são feitas entrevistas com um guião formulado para resposta dos entrevistados. Na presente dissertação foi pedido aos entrevistados que dessem a sua opinião baseada na sua experiência profissional, extremamente pertinente para o caso em estudo sobre três afirmações diretamente relacionadas com as hipóteses de investigação.

Foi pensado envolver determinadas personalidades relevantes para o estudo ligadas à verificação da compliance com o RGPD. Temos opinião de dois especialistas na temática da proteção de dados pessoais. Uma encarregada de proteção de dados, com formação em diversas áreas do direito, que desenvolve ações de formação e consultoria sobre o RGPD em diversas organizações de várias dimensões. E a análise conta também com um profissional portador de uma vasta formação em diversas áreas incluindo o direito, auditoria interna, proteção dados, fraude e risco, com um vasto currículo e que desenvolve atualmente funções de auditoria e compliance com o RGPD.

A) A primeira afirmação pedia que o inquirido comentasse o impacto e necessidade de moldagem das organizações face ao cumprimento com o RGPD e existência de uma perceção de conhecimento efetivo ainda limitado sobre o regime: "O RGPD trouxe grande impacto, necessidade de adaptação e moldagem nas organizações, existindo ainda conhecimento limitado sobre o mesmo."

B) A segunda afirmação foi de encontro com o comentário sobre a existência de pouco conhecimento da figura do EPD nas organizações e a necessidades de formação do mesmo: "O EPD é uma figura ainda pouco conhecida e com necessidades de formação."

C) A última observação vai de encontro ao comentário sobre o contributo da auditoria, interna e de conformidade para a compliance com o RGPD: "A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD."

3 Apresentação Caso Empírico

Nesta fase, já foram obtidas as respostas necessárias para serem trabalhados os resultados e procedermos à apresentação dos mesmos de acordo com uma análise criteriosa para posterior conclusão sobre o estudo.

3.1 Apresentação e interpretação dos resultados

3.1.1 Resultados da análise quantitativa

Antes de começar a análise dos resultados é importante ressalvar que, foi pedido a todos os inquiridos tivessem em consideração para a resposta, a empresa para a qual trabalham (no caso, conforme já mencionado, as empresas do PSI-20).

A tabela seguinte sintetiza todos os resultados obtidos do questionário de acordo com a escala utilizada, são ainda identificadas as questões que correspondem a cada hipótese.

Tabela 4 - Escala de resposta e Hipóteses

	Hipótese 1						**Hipótese 2**			**Hipótese 3**	
Questões / Escala	**Q.4**	**Q.5**	**Q.6**	**Q.7**	**Q.8**	**Q.9**	**Q.10**	**Q.11**	**Q.12**	**Q.13**	**Q.14**
Discordo	0%	5%	0%	80%	10%	5%	5%	20%	0%	0%	10%
Nem concordo nem discordo	0%	0%	5%	10%	15%	45%	10%	25%	25%	45%	20%
Concordo em parte	40%	70%	50%	10%	50%	45%	15%	50%	20%	20%	15%
Concordo totalmente	60%	25%	45%	0%	25%	5%	70%	5%	55%	35%	55%

Relembrado a primeira Hipótese de investigação, temos:

H1: As organizações conhecem o RGPD, mas este, trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas.

Para podermos analisar a veracidade da Hipótese 1 selecionamos a questões de 4 a 9 do questionário.

Tabela 5 - Questões para Hipótese 1

Q.4	Tem conhecimento dos temas abordados pelo RGPD (Regulamento geral de proteção de dados?)
Q.5	Considero que a empresa se encontrava preparada quando o RGPD passou a ser obrigatório, proporcionando os recursos necessários e adotando medidas adequadas (Políticas, processos internos).
Q.6	Considero que o impacto do regulamento na empresa foi minimizado, dado que existiu uma consciencialização geral sobre a privacidade e proteção de dados dentro da organização.
Q.7	O tema tem sido "adiado" e não existe até então alterações significativas de processos, não sendo percebida muita preocupação e abertura para aplicação deste regulamento.
Q.8	Considero que este regulamento alterou substancialmente a forma de trabalho, trazendo várias preocupações, procedimentos adicionais e alterando vários processos existentes.
Q.9	A adoção de novas práticas á luz do RGPD trouxe melhores resultados ao nível de satisfação de clientes/funcionários/melhoramento de processos e menor utilização de recursos.

Fonte: Elaboração própria (2020)

Começando pela quarta questão 60% dos inquiridos consideram que estão em posição de "concordar totalmente" com a afirmação. Apesar da maioria estar à vontade com os temas abordados pelo RGPD, uma percentagem considerável da amostra (40%), apenas "concorda em parte" quando a este conhecimento, ainda assim, o regime não é considerado como desconhecido.

A escolha especifica dos "temas abordados" pretendia saber, não só se o regime é conhecido de forma genérica pelos profissionais questionados, mas também para além disso, se os temos efetivamente abordados são conhecidos, e talvez por essa referência a percentagem seja em parte de respostas não concordantes na totalidade.

No que diz respeito à quinta questão, as respostas na sua maioria (70%) vão de encontro com uma concordância parcial, ou seja, 70% das pessoas inquiridas considera que a empresa não estava totalmente preparada quando o regime passou a ser obrigatório e havia trabalho a desenvolver nesta matéria. Apesar desta maioria, 25% concordam

totalmente com afirmação traduzindo a total preparação para adoção do regime por parte das empresas para as quais trabalham. Apenas 5% discordaram da afirmação, demonstrando a total falta de preparação e falha nas medidas que deveriam ter sido tomadas à data.

Na seguinte questão a ideia é perceber o impacto percebido na organização, de acordo com as medidas preventivas que foram (ou não) tomadas. É percebida nesta questão uma divisão na resposta por parte dos inquiridos (50% concordou em parte, 45% concordou totalmente, 5% não tem opinião). Vamos primeiramente virar a nossa atenção para as respostas que traduzem uma boa performance das empresas quanto à consciencialização da privacidade e minimização de impacto, dado que em 45% a concordância é total. Contudo 50% dos inquiridos concorda só em parte, o que deixa margem para percebermos que o impacto esteve presente e a consciencialização e políticas internas ficaram aquém do esperado.

É na questão nº7 que é percebida uma concordância esmagadora em discordar. 80% dos inquiridos discordam que o tema tem sido "adiado" dentro da organização, que não existiram alterações de processos ou que existiu falta de preocupação com a temática. Apenas 10% concordaram em parte e 10% não demonstram opinião. Com as respostas a esta questão é percebido claramente que existiram alterações significativas no caminho para a compliance com o RGPD e que, na sua grande maioria, não é percebida pouca importância dada ao tema, pelo contrário sendo percebida preocupação.

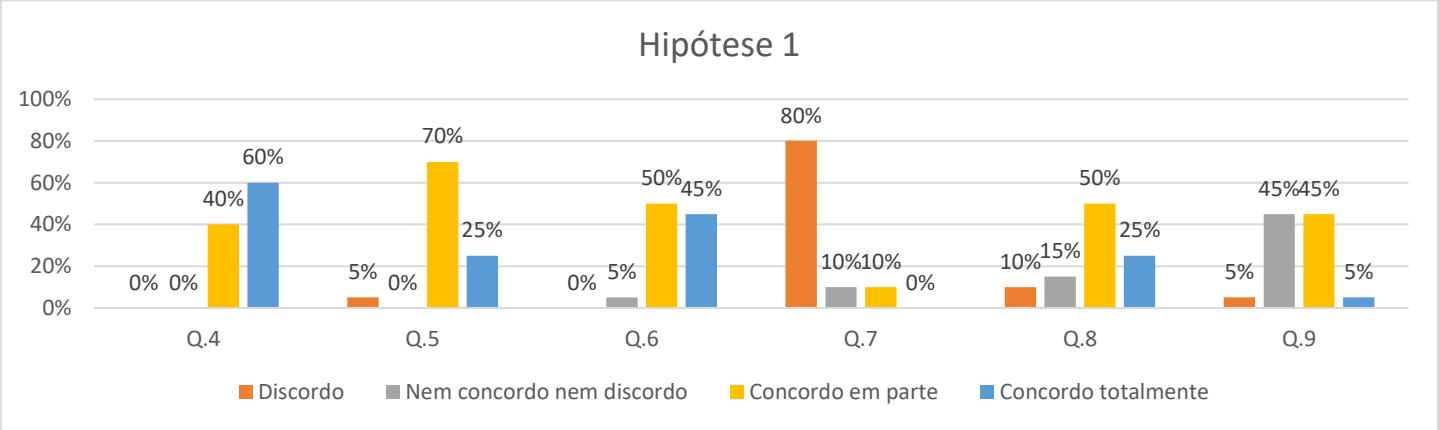
Constatamos uma dispersão entre as 4 opções de resposta na questão nº8 do questionário. Com esta questão pretendemos tentar perceber o nível de constrangimento, procedimentos adicionais, alteração da forma de trabalho que este regime trouxe. E temos 50% de respostas "concordo em parte" para alteração substancial da forma de trabalho (seja por novas tarefas ou atualização/revisão de processos existentes). A restante percentagem de respostas divide-se entre discordo (10%), nem concordo nem discordo (15%), e concordo totalmente (25%).

Quanto á questão nº9, que tinha como objetivo perceber se a organização tirou vantagem com a adoção do regime ao nível de satisfação de clientes/funcionários e melhor funcionamento de processos a nível interno, os inquiridos demonstram falta de conhecimento sobre isso (45% nem concorda nem discorda). No entanto mais 45% concorda em parte que existiram melhorias nesse sentido, e 5%+5% ficaram no concordo

totalmente e discordo. Apesar das diferentes opiniões podemos perceber que em parte as organizações tiraram partido das novas obrigações a cumprir em matéria de RGPD.

De seguida é apresentado o quadro resumo com a relação das percentagens obtidas por questão para a hipótese 1.

Figura 9 - Respostas questionário H1



Fonte: Elaboração própria (2020)

Relembramos agora a segunda hipótese de investigação em estudo, que nos centra a atenção para uma das figuras mais importantes do RGPD, o encarregado de proteção dados:

H2: O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.

Para esta hipótese foram elaboradas as seguintes questões para resposta no questionário:

Tabela 6 - Questões para Hipótese 2

Q.10	Tenho conhecimento que existe encarregado proteção de dados na empresa ou desempenho essa mesma função.

Q.11	Considero a temática bastante complexa, e sinto necessidade de formação profissional ou informação de esclarecimento sobre o tema.
Q.12	Considero que o encarregado de proteção de dados tem as competências profissionais necessárias e pertinentes para desempenhar as suas funções.

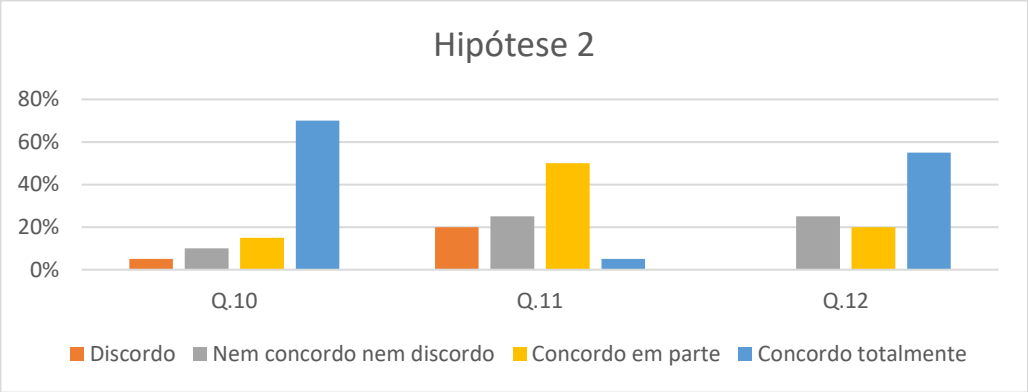
Fonte: Elaboração própria (2020)

Na questão 10, a maioria (70%), não teve dúvidas que tem conhecimento da existência do EPD. Ainda assim, dado que os questionários foram direcionados a pessoas que tratam dados no âmbito da sua atividade profissional, além de EPD ou responsáveis pela compliance, é de salientar que 15% não tem total conhecimento, e consideramos os 15%+5% de nem concordo nem discordo e discordo respetivamente como desconhecimento da figura do encarregado de proteção de dados.

Na questão nº11, apenas 5% dos inquiridos admitem que se trata de um tema bastante complexo e sentem que precisam de formação/informação adicional. Em posição diferente encontram-se 50% dos inquiridos que revelam concordar em parte na falta de formação profissional e informação de esclarecimento que sentem sobre este regulamento, assim como, a elevada complexidade associada a este tema. Foi pensado questionar formação profissional (mais adequado a profissionais como os EPD em que é imperativo o conhecimento do direito, nomeadamente as disposições legais no âmbito do RGPD, e práticas de proteção de dados), e informação adicional (mais adequada aos restantes profissionais porque apesar da preocupação com o cumprimento legal também ser importante, procuram esclarecimentos mais específicos sobre determinado procedimento).

Inevitavelmente para resposta à questão nº12 é necessário ter algum conhecimento do EPD e das funções desempenhadas pelo mesmo. Foi então pedido que a reflexão nesta questão, fosse no sentido de expressarem a sua opinião sobre a competência profissional do EPD. Nesta questão ninguém põe em causa esta competência (obtendo-se 0% para discordo), mas 25% nem concordam nem discordam, que nos traduz uma posição de falta de conhecimento de causa. E as respostas positivas também se destacam nesta questão, com 20% de concordo em parte e 55% de concordo totalmente. Para a hipótese 2 o gráfico ilustrativo do panorama apresenta-se de seguida:

Figura 10 - Respostas questionário H2



Fonte: Elaboração própria (2020)

Relembramos agora a nossa terceira e última hipótese, que relaciona o RGPD com a auditoria:

H3: A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.

Existiram 2 questões no questionário dedicadas a esta hipótese e são as seguintes.

Tabela 7 - Questões para Hipótese 3

Q.13	O trabalho realizado pelas auditorias de conformidade no âmbito do RGPD (externas) ajuda à clarificação de temas, fornece sugestões de melhoria e apoia na adoção de novos procedimentos.
Q.14	A auditoria interna tem um papel ativo no apoio ao cumprimento do RGPD, assumindo papel preponderante na gestão de riscos e definição de controlos.

Fonte: Elaboração própria (2020)

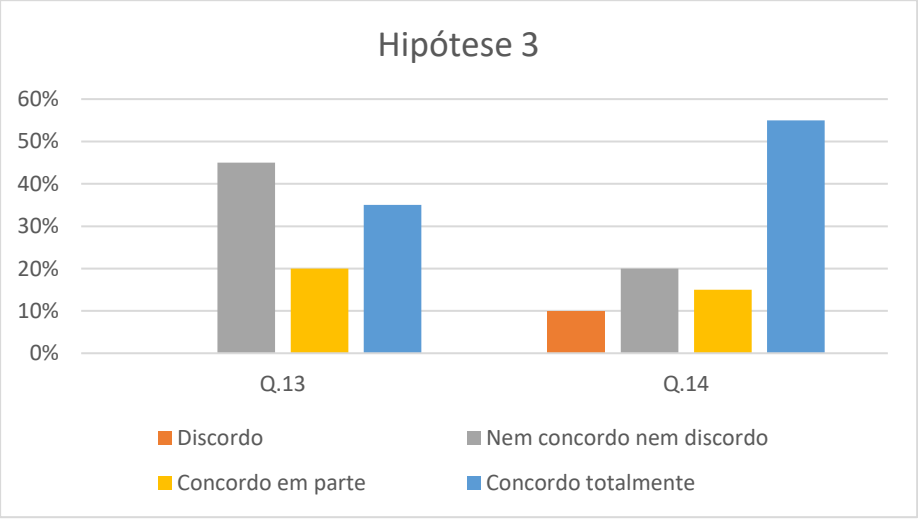
Quando inserimos o tema auditoria, a auditoria externa destaca-se por não serem tão conhecidos ou talvez evidentes os seus contributos para a conformidade com o RGPD. E é isto mesmo que nos comprovam as respostas à questão nº13, 45% das respostas cai

sobre a opção "nem concordo nem discordo". Mas é percetível que uma grande parte dos inquiridos na amostra considera que a clarificação de temas, sugestões e o apoio em decisões futuras se traduz como vantagem nas auditorias de conformidade com o RGPD. Uma vez que, 20% dos inquiridos concordam na parte com a afirmação e 35% concordam totalmente, perfazendo 55% de respostas favoráveis.

No que à auditoria interna diz respeito, o seu apoio para cumprimento do RGPD, assim como, o papel de auxílio na gestão de riscos e definição de controlos é defendido na totalidade por 55% dos inquiridos, somando a estes 15% que concordaram em parte. Existe uma pequena percentagem de respostas desfavoráveis a esta teoria benéfica de auxílio de auditoria interna, sendo esta de 10% de discordância com o papel ativo da auditoria interna. Ainda uma percentagem de 20% revelam, também de acordo com o verificado na questão anterior, desconhecimento dos contributos da auditoria interna na conformidade e auxílio com a implementação do RGPD.

Traduzindo os resultados obtidos em gráfico, obtemos a seguinte representação:

Figura 11 - Respostas questionário H3



Fonte: Elaboração própria (2020)

Para averiguação da veracidade das três hipóteses em estudo foi elaborada a tabela apresentada de seguida. A tabela apresenta-nos as questões dedicadas a cada hipótese de investigação e seguidamente a predominância de cada questão para a primeira hipótese.

Foi decidido inserir na tabela o nível de concordância a discordância para cada questão. Foi necessária esta inclusão uma vez que, para validação da Hipótese em certas questões o que nos é interessante avaliar é a discordância e não concordância (Questão nº7 para a primeira hipótese). No final apresenta-se a percentagem de aprovação obtida para cada uma das hipóteses.

Tabela 8 - Aprovação das Hipóteses em estudo

Hipóteses	Questões	Predominância p/ Questão (%)	Concordância c/ Questão	Discordância c/ Questão	Verificação da Hipótese
H1	**Q.4**	16.6(6)	100%	0%	**83%**
	Q.5	16.6(6)	95%	5%	
	Q.6	16.6(6)	95%	0%	
	Q.7	16.6(6)	10%	80%	
	Q.8	16.6(6)	75%	10%	
	Q.9	16.6(6)	50%	5%	
H2	**Q.10**	33.33(3)	85%	5%	**72%**
	Q.11	33.33(3)	55%	20%	
	Q.12	33.33(3)	75%	20%	
H3	**Q.13**	50	55%	0%	**63%**
	Q.14	50	70%	10%	
			Aprovação das hipóteses de análise		**72,6%**

Fonte: Elaboração própria (2020)

Tendo agora o cálculo final das respostas obtidas, podemos verificar que no todo as hipóteses e consequentemente o modelo estão comprovadas em 72% (sendo que as hipóteses valem igualmente em termos de percentagem no modelo: 33.33%).

3.1.2 Resultados da análise qualitativa

Conforme explicado anteriormente, apresentam-se de seguida as respostas obtidas quanto ao pedido de comentário sobre cada temática.

3.1.2.1 Respostas obtidas Inquirido I

A) O RGPD trouxe grande impacto, necessidade de adaptação e moldagem nas organizações, existindo ainda conhecimento limitado sobre o mesmo.

A resposta obtida foi a seguinte:

"O RGPD obrigou muitas entidades a alterarem procedimentos e teve grande impacto na atividade daquelas que passaram por um procedimento de adequação e implementação. Desde eliminação de documentos, como processos de informatização, investimento em tecnologia e em equipamentos (ex: armários com fechadura, trituradoras de papel, etc), até ações de sensibilização do pessoal em relação a violações de dados pessoais e confidencialidade. Apesar de ser uma preocupação de muitas entidades, assiste-se a implementações deficientes ou mesmo erradas (como cláusulas de consentimentos dos colaboradores a serem aditadas aos respetivos contratos de trabalho), pelo que se pode dizer que o conhecimento generalizado, está ainda um pouco aquém do que se pretende. Dai a importância da aposta na formação e na contratação de profissionais especializados na matéria."

B) O EPD ainda é uma figura ainda pouco conhecida e com necessidades de formação.

A resposta obtida foi a seguinte:

"O EPD começa já a ser uma figura conhecida, até porque a sua existência no seio de algumas organizações é obrigatório. No entanto, na prática assiste-se a inúmeros EPDs nomeados sem cumprirem os requisitos do art.º 37.º, n.º 5 do RGPD ("conhecimentos especializados no domínio do direito e das práticas de proteção de dados"). Assistimos a vários casos de EPDs que são colaboradores da própria entidade, exercendo

cumulativamente funções de como administrativos, por exemplo. Nesses casos, será evidente a necessidade de formação específica na área da proteção de dados, uma vez que a formação base, à partida não será adequada nem suficiente.

Mais grave ainda é o caso de Diretores de Recursos Humanos ou de Departamentos de Segurança Informática, por exemplo, ou até, em alguns casos de PME´s – o próprio sócio gerente. Esta realidade evidencia uma falta de informação generalizada ou mesmo uma negligência das entidades, em nomear um EPD junto da CNPD ou para "inglês ver", sendo que esses casos violam completamente o dever de isenção e independência a que o DPO está adstrito, bem como pode potenciar conflitos de interesses. O preferível será sempre contratar em "outsourcing".

C) A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.

A resposta obtida foi a seguinte:

"De facto, as auditorias são imprescindíveis para se manter o compliance, uma vez que envolvem uma fase de diagnóstico e permitem a recomendações de medidas específicas e casuísticas em relação à organização. A auditoria inicial de adequação ao RGPD tem um papel primordial, sem descurar a importância das auditorias posteriores e periódicas, uma vez que a situação das entidades é volátil e poderão surgir sempre novas operações de tratamentos de dados, tanto resultantes de mudanças de procedimentos internos, como resultantes de eventuais alterações legislativas. Também o papel do DPO nestas auditorias se revela fulcral, nos termos do art.º 11.º, al. a) da Lei 58/2019 (lei de execução do RGPD) e do art.º 39.º, n.º 1, al. b) do RGPD. Para além disso, os relatórios subjacentes às próprias auditorias são um bom exemplo de cumprimento."

3.1.2.2 Respostas obtidas Inquirido II

A) O RGPD trouxe grande impacto, necessidade de adaptação e moldagem nas organizações, existindo ainda conhecimento limitado sobre o mesmo.

A resposta obtida foi a seguinte

"O tema da privacidade em Portugal não é recente. Podemos encontrar este tema na Constituição de 1976, assim como em vária legislação que se seguiu. Portugal tem, por exemplo uma autoridade de controlo a CNPD já com muitos anos de actividade. Por exemplo o Brasil, que implementou agora uma lei de proteção de dados, a JGPD, apenas agora criou uma autoridade de controle. A antiga lei de proteção de dados, que derivava de uma diretiva europeia já era de conhecimento das organizações e de adaptação destas a essa realidade jurídica, principalmente as grandes empresas. Claro está que o RGPD com a implementação de coimas elevadas obrigou as organizações a um outro estádio de conformidade e isso naturalmente suscitou outro tipo de ajustamentos e claro de impactos. Desde 2016 muita informação foi prestada acerca deste tema e as organizações, quer em Portugal quer no resto da Europa souberam adaptar-se. Claro está mais umas do que outras. Eu diria que as grandes empresas o fizeram facilmente (porque já o tinham feito no âmbito da legislação anterior), as PME´s fizeram um grande esforço de acompanhamento, quer em termos humanos quer financeiros, as pequenas empresas fizeram pouco, acharam que não se lhes aplicava ou que não se lhes aplicava muito…
Com a informação que correu em toda a Europa creio ser difícil afirmar que as organizações têm um conhecimento limitado. Podem ter sim uma vontade limitada de conhecer."

B) O EPD ainda é uma figura ainda pouco conhecida e com necessidades de formação.

A resposta obtida foi a seguinte

"Concordo com esta afirmação. Nos seus dois sentidos. É uma figura pouco conhecida em termos gerais e em termos particulares. O grande público sabe muito pouco sobre esta figura, o que faz, o que pode fazer, a sua necessidade nas organizações etc. Infelizmente

também nas organizações onde essa figura é criada existe um grande desconhecimento sobre os seus poderes. A gestão das organizações tem nomeado DPO, por necessidade, por moda ou por modernice sem perceberem exatamente o que estão a criar, as suas competências, os seus direitos, as suas obrigações e principalmente a sua posição na organização. Assistiu-se à nomeação para este cargo de pessoas que simplesmente estavam "à mão" nas organizações, fossem elas juristas, economistas, informáticos, ou seja sem um critério que se baseasse naquilo que efetivamente o RGPD determina. Foi pena, podia-se ter criado uma nova classe profissional empenhada na proteção dos dados pessoais as pessoas que interagem com as suas organizações, e infelizmente, verificou-se a criação de um cargo mais preocupado em defender as próprias organizações, o que se verificaria, de qualquer modo se se defendesse principalmente os dados pessoais de quem interage com as organizações."

C) A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.

"A conformidade é um processo. Nunca é definitiva. As organizações precisam de verificar, a todo o tempo, o "estado da arte". O próprio RGPD impõe ao DPO a realização de auditorias sistemáticas. Uma organização pode achar que está em conformidade hoje e, logo no dia seguinte, se tiver um problema de segurança e não proceder ao estabelecido no regulamento em termos de procedimentos de informação, já não está conforme.
As auditorias sejam elas efetuadas in *house* ou recorrendo a entidades externas asseguram o controle desse processo, ou pelo menos demonstram a vontade de assegurar esse processo, e isso é particularmente importante nas situações de falha da organização e nomeadamente na medida da coima que poderá ser estabelecida pela autoridade de controle."

3.1.3 Confronto resultados obtidos

Confrontando os resultados obtidos na análise qualitativa e quantitativa, apresenta-se o seguinte esquema.

<table>
<tr><td>Hipótese 1: As organizações conhecem o RGPD, mas este, trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas.</td><td>Principais conclusões análise quantitativa:
⇨ RGPD é conhecido nas organizações;
⇨ Benefício da preparação
⇨ Grande impacto causado: necessidade de medidas adicionais
⇨ Preocupação para a compliance evidente: Não houve lugar a políticas de “deixa andar”
⇨ Evidentes alterações na forma de trabalho
⇨ Vantagem a nível de satisfação clientes/funcionários/melhoramento processos não é claramente defendida</td></tr>
<tr><td colspan="2">Opinião obtida na análise qualitativa comprova resultados obtidos:
⇨ Conhecimento existe ainda que implementações aquém do esperado, preocupação também existente por parte das organizações.
⇨ Grande e claro impacto na atividade das empresas que se adequaram e implementaram o RGPD</td></tr>
<tr><td>Hipótese 2: O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.</td><td>Principais conclusões análise quantitativa:
⇨ EPD conhecido na organização de forma geral
⇨ Reconhecida a sua competência profissional
⇨ Desconhecimento sobre necessidade de formação/informação, mas maioria admite estas necessidades</td></tr>
<tr><td colspan="2">Opinião obtida na análise qualitativa não comprova resultados obtidos:
⇨ Necessidade de formação; nomeações deficientes de EPD, conhecimento vago sobre esta figura</td></tr>
</table>

<table>
<tr>
<td>Hipótese 3: A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.</td>
<td>Principais conclusões análise quantitativa:
⇨ Hipótese validada em percentagem inferior às anteriores
⇨ Benefício da auditoria interna destacado, nomeadamente na gestão de riscos e definição de controlos.
⇨ Benefícios para auxílio, clarificação e suporte em relação ao RGPD também admitidos para a auditoria externa, ainda que, não tão defendidos.</td>
</tr>
<tr>
<td colspan="2">Opinião obtida na análise qualitativa comprova resultados obtidos
⇨ Ambas devem ser realizadas de forma sistemática
⇨ Ambas as auditorias se traduzem como imprescindíveis na demonstração e controlo constante do compliance com o RGPD</td>
</tr>
</table>

Para Prodanov e Freitas (2013) nesta última fase "retomamos o problema inicial", é necessário fazer uma nova avaliação dos resultados obtidos e confrontar com o objetivo do estudo e questões levantadas.

No capítulo I (Revisão da literatura), procedeu-se a explicação de todos os tópicos pertinentes no âmbito deste estudo. No capítulo II (Metodologia) foi apresentada a forma como o estudo ia ser conduzido e os métodos a utilizar na recolha de dados. E o Capítulo III (Caso Impírico), traduziu-se na apresentação dos resultados obtidos com algumas considerações pré conclusões finais.

Se por um lado o RGPD ofereceu maior segurança e proteção individual dos direitos pessoais sobre a privacidade, aumentou a responsabilidade das organizações que recolhem, tratam e armazenam esses dados.

Face a todas as mudanças inerentes à implementação deste Regulamento, obrigatório em alguns casos e no geral sempre recomendado, relembramos o objetivo proposto para estudo inicialmente. Era então pretendido perceber o nível de conhecimento do regime por parte das organizações, assim como, os constrangimentos e implicações que este acarretou, ou se até foram percebidos beneficios. Compreender também a perceção sobre o EPD e suas funções. E por último era objetivo somado aos anteriores perceber o contributo das audorias realizadas neste âmbito.

Tal como já explicado anteriormente atribuiu-se o valor de 1/3 para cada uma das três hipóteses em estudo da problemática também já explicitada.

Foi obtida a percentagem de 83%, em média, no conjunto das questões enquadradoras da Hipótese 1 na análise quantitativa: **As organizações conhecem o RGPD, mas este trouxe grande impacto e necessidades de adaptação, sendo minimizados nas empresas melhor preparadas**. O que aponta para que no final deste estudo seja percebido que O RGPD é conhecido nas organizações em estudo (as que compõe o PSI-20). As empresas que se encontravam melhor preparadas, quer a nível de formação, nomeação de pessoal qualificado na temática, estudo realizado sobre o Regulamento, desenvolvimento de políticas e processos internos tiraram partido disso. Ainda que assim seja, os resultados revelam que o impacto causado pelo regulamento esteve presente, e que as medidas na maior parte das empresas em estudo não foram suficientes, sendo que, 70% dos inquiridos considera que a empresa não estava totalmente preparada quando o regime passou a ser obrigatório. No que respeita ao caminho realizado para a compliance

com o RGPD é claro que existe preocupação, o tema não foi de todo "adiado" tal como questionado, muito pelo contrário, permitindo concluir que foram evidentes as alterações significativas neste sentido. O regulamento trouxe alteração na forma de trabalho, sendo que não foi atribuída alteração significativa na totalidade, processos adicionais existiram assim como, novas preocupações que obrigaram a alteração dos métodos de trabalho em alguns aspetos. No que diz respeito aos benefícios trazidos pela a adoção do regime ao nível de satisfação de clientes/funcionários/melhoramento de processos e menor utilização de recursos, a perceção dos inquiridos não é clara. Este ponto é desconhecido por aproximadamente metade das pessoas envolvidas. A tendência dos restantes 50% recai para a admissão de que que em parte as organizações tiraram partido das novas obrigações a cumprir em matéria de RGPD, e de que a adoção de novas práticas neste sentido trouxe vantagem.

A opinião obtida na análise qualitativa, comprova totalmente o grande e claro impacto na atividade das empresas que se adequaram e implementaram o RGPD, com a consequente alteração de procedimentos e necessidade de ajustamentos. É admitida também a preocupação existente por parte das entidades, um dos inquiridos considera que o conhecimento generalizado com toda a informação disponível não pode ser considerado limitado. No entanto, o segundo inquirido complementa que este se encontra aquém do que se pretende devendo apostar-se na formação e contratação de profissionais especializados na matéria. Ambos os comentários seguem no sentido de conhecimento existente, necessidade de esforço adicional e inegável impacto.

Resumidamente, as conclusões gerais tiradas para comprovação da Hipótese 1 revelam que, as organizações conhecem o RGPD e desenvolveram esforços no sentido da compliance com o mesmo. Este revelou grande impacto nas organizações, sendo percebida alguma falta de preparação e que ainda há trabalho a ser feito neste âmbito. Pelo lado positivo, os efeitos foram diminuídos quando existiu preparação sobre algum procedimento e também existem benefícios na adoção destas novas práticas.

Passando para a Hipótese 2, foi obtida a percentagem de 72%, em média, na análise quantitativa: **O EPD é conhecido na organização e qualificado para o cargo, mas com necessidades de formação.** Conclui-se, portanto, que, na sua grande maioria o EPD é conhecido dentro das organizações em estudo. No entanto, dado que os questionários foram direcionados a pessoas que tratam dados no âmbito da sua atividade profissional é surpreendente que esta percentagem não se traduza os 100% de conhecimento desta figura

tão importante introduzida pelo RGPD. Conclui-se também que é reconhecida a competência profissional do EPD para o desempenho das suas funções. A necessidade de formação profissional ou informação adicional de esclarecimento sobre o regulamento é admitida na maioria embora com opiniões de percentagem significativa no sentido contrário em discordância e também desconhecimento de causa.

Confrontando as conclusões anteriores com a opinião dada na análise qualitativa, o conhecimento do EPD demonstra-se como não comprovado. Aqui a opinião é mais criteriosa e percetível quanto à falta de formação específica e adequada na área. Havendo lugar por vezes a conflitos de interesse e comprometimento da independência e isenção exigida pelo RGPD, dado que os nomeados para encarregados pela proteção de dados muitas vezes são colaboradores da própria entidade com outras funções acumuladas. Para o segundo inquirido o conhecimento quer em teros gerais, quer em termos particulares do DPO é ainda pouco. Quanto ao verdadeiro conhecimento a opinião nesta análise defende claramente como sendo ainda muito vago opondo-se em parte à conclusão obtida anteriormente na análise quantitativa.

Conclui-se resumidamente face a esta segunda Hipótese de investigação que o EDP é uma figura em termos de existência que vai sendo conhecida, mas não em temos de: como opera, as suas funções e responsabilidades ou a necessidade de existência deste. São atribuídas a este as competências profissionais necessárias, existindo várias necessidades adicionais formação e esclarecimentos generalizados sobre o RGPD a todos os envolvidos em processos e tratamento de dados pessoais. A necessidade de formação é fortemente defendida por ambos, assim como, deficiências existentes no processo de nomeação deste profissional quando necessário.

A Hipótese 3 revela 63%, em média, de comprovação com as questões na análise quantitativa: **A auditoria interna e externa (de conformidade) traduzem-se em apoios essenciais para a compliance com o RGPD.** Esta hipótese é a menos válida para o público inquirido, e é nesta hipótese que se revela também maior desconhecimento de causa. Os benefícios na ajuda na clarificação de temas, fornecimento de sugestões de melhoria e apoio por parte da auditoria externa (de conformidade) são defendidos e comprovados pelo público inquirido. Por sua vez a auditoria interna revela ser mais útil e eficaz quanto ao seu contributo na conformidade e auxílio com a implementação do RGPD, nomeadamente na gestão de riscos e definição de controlos.

Na análise qualitativa a opinião sobre as auditorias de conformidade com RGPD revela-se mais destacada, sendo que é defendido que todas auditorias são imprescindíveis para se manter o compliance. Sendo defendido que a "conformidade é um processo", estas auditorias, internas ou externas, devem ser realizadas constantemente de forma a garantir essa mesma conformidade e a demonstrá-la.

Na terceira e última hipótese podemos concluir que ambas as auditorias se traduzem como imprescindíveis na demonstração e controlo constante do compliance com o RGPD.

Após estudadas as três hipóteses, a validação final do modelo de análise verifica-se em 72%. Esperava-se comprovar as teorias (hipóteses) inicialmente formuladas, o que se veio a comprovar positivamente dada a percentagem de validação final obtida.

Para além dos resultados e conclusões obtidas sobre o regulamento nas organizações em estudo, podemos concluir que ao longo dos anos a importância pela privacidade começou a adquirir maior ênfase no panorama do direito europeu e internacional. Com as mutações constantes no desenvolvimento da sociedade atual e nas tecnologias de informação, esta á cada vez mais uma das grandes preocupações a nível mundial. A proteção dos nossos dados pessoais, na disponibilização, tratamento ou armazenamento é hoje em dia vista com outros olhos e cada vez mais caminha para uma maior consciencialização e preocupação individual e coletiva.

O regulamento 2016/679 do parlamento europeu e do conselho de 27 de abril, assegurado na ordem jurídica nacional pela LNE 58/2019, veio revolucionar a vida nas organizações. Aplica-se em organizações estabelecidas na UE e fora desta desde que estejam a processar dados pessoais de residentes na UE (sejam referentes a bens, serviços ou controlo de comportamento de pessoas). Neste contexto surge o encarregado de proteção de dados, figura destacada neste âmbito que deve desempenhar as suas funções com autonomia e independência, obrigado ao dever de sigilo e confidencialidade. Este tem, pelo menos, funções de informação e aconselhamento de todo o responsável por tratamento dos dados ou subcontratante. Sabendo que, cabe as organizações demonstrar conformidade com o RGPD as AIPD são essenciais e devem ser realizadas antes de iniciar qualquer tratamento dos dados e continuamente de acordo com a periodicidade necessária, assim como as auditorias de conformidade. As consequências de incumprimento são severas, podem advir responsabilidades criminais, civis ou contraordenacionais. Em conjunto a autoridade de controlo nesta matéria (CNPD) pode ainda aplicar sanções acessórias se

assim o entender. O incumprimento poderá implicar multas até os 20M€ ou 4% do volume de negócios.

Limitações do estudo

Ao longo desta pesquisa algumas dificuldades foram sendo encontradas tornando-se em limitações do estudo. As primeiras limitações foram encontradas na revisão da literatura, dado que o tema escolhido é ainda relativamente recente, e o regulamento em causa passou a ser obrigatório apenas em 2018, foi difícil encontrar artigos e trabalhos desenvolvidos sobre a temática para poder investigar estudos anteriormente feitos. A maior limitação foi a obtenção de resposta aos questionários, foi extremamente dificil obter respostas das empresas que estavam enquadradas neste estudo, sendo que algumas das empresas inquiridas não colaboraram com o preenchimento do mesmo. Contudo e face á amostra reduzida de empresas escolhidas no âmbito do estudo foi possível tirar as conclusões pretendidas. Foi ainda uma limitação o facto de os questionários serem anónimos, apesar de uma preocupação que assim fosse, não permitiu que fossem acompanhadas as respostas consoante as empresas, mas sim o cargo no geral.

Pistas para investigação futura

Por último, sugere-se para investigações futuras que seja feito o estudo em empresas de dimensão mais reduzidas (em PMEs por exemplo), dado que o panorama em matéria de RGPD se prever ser diferente das empresas que compõe o PSI-20, além de que se traduzem num número mais considerável de profissionais a serem inquiridos, e além dos profissionais incluídos neste estudo somar os profissionais responsáveis pelos sistemas de informação na organização. Será mais interessante realizar o estudo a um número maior de inquiridos. Também seria interessante a comparação entre setores de atividades diferentes, de modo a perceber as diferenças em matéria de conformidade com o RGPD. Aquando a realização do tratamento dos resultado obtidos foi-se percebendo que algumas questões colocadas em ambas as análises poderiam ter ido mais de encontro às hipóteses de forma a validação se tornar mais fácil e claro, sugerimos que isto em investigações futuras este pormenor seja bem pensado antecipadamente.

Antunes, L. (2018). Pôr em prática o RGPD. O que muda para nós? E para as organizações? (1ªedição). Lisboa: FCA

Baptista, C. & Sousa, M. (2011). Como fazer investigação, dissertações, tese e relatórios segundo Bolonha (2ª edição). Lisboa: Pactor

Coutinho, C. (2013). Metodologia de investigação em ciências sociais e humanas (3ª edição). Porto: Edições Almedina

Cunha, D., Silva, D. & Hierro, A. (2020). Guia do processo de adequação ao regulamento geral de proteção de dados. Implementação e auditoria (1ªedição). Porto: Edições Almedina

Fazendeiro, A. (2018). Regulamento geral sobre a proteção de dados. Algumas notas sobre o RGPD (3ª edição). Porto: Edições Almedina

Magalhães, F. & Pereira, M. (2018). Regulamento geral de proteção de dados manual prático (2ª edição). Porto: Vida Económica

Pedrosa, A. & Gama, S. (2016). Introdução computacional à probabilidade e estatística com Excel (3ª edição). Porto: Porto Editora

Prodanov, C. & Freitas, E. (2013). Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho académico (2ªedição). Brasil: Universidade Feevale

Saldanha, N. (2019). RGPD Guia para uma auditoria de conformidade (1ª edição). Lisboa: FCA

Vilelas, J. (2017). Investigação: O processo de construção do conhecimento (2ª edição). Lisboa: Edições Sílabo

Dissertações

Ribeiro. F (2017). Dissertação de especialidade em Ciências Jurídico-Políticas O Tratamento de dados pessoais de clientes para marketing, Universidade Autónoma de Lisboa.

Vaz, A (2018). Dissertação em Ciências Jurídico-Forenses: O Regulamento Geral de Proteção de Dados: Desafios e Impactos, Faculdade de direito da Universidade de Coimbra

Vieira, T. (2007). Dissertação em Direito: O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação, Universidade de Brasília

Cruz, A. (2019). Dissertação de mestrado em auditoria: O impacto do controlo interno nas PME excelência, Instituto superior de contabilidade e administração do porto

Lopes, I. (2019). Dissertação de mestrado em auditoria: A ética e a opinião do auditor, Instituto superior de contabilidade e administração do porto

Correia, R. (2015). Dissertação de mestrado em auditoria: Auditoria de recursos humanos nas PME Portuguesas. Instituto superior de contabilidade e administração do porto

Ferreira, C. (2019). Dissertação de mestrado em solicitadoria de empresa: A monotorização do trabalhador e o RGPD, Escola superior de tecnologia e gestão

Mendes, P. (2018). Dissertação de mestrado em segurança informática: Análise de risco no GDPR, Faculdade de ciências da Universidade de Lisboa

Legislação

Carta dos direitos fundamentais da União europeia (2016/C 202/02)

Código do trabalho

Comissão ao Parlamento Europeu, ao Conselho, o Comité Económico e Social e o Comité das Regiões - "Uma abordagem abrangente sobre a proteção de dados pessoais na União Europeia".

Diretiva 95/45/CE do parlamento europeu e do conselho de 24 de outubro de 1995

ISO 31000:2009 Gestão do Risco

Lei de execução 58/2019 de 8 de agosto, diário da república 1ª série

Parecer da autoridade Europeia para a Proteção de dados sobre a comunicação da

Parecer 05/2014 de 10 de abril de 2014 sobre técnicas de anonimização

Parecer 04/2007 de 20 de julho sobre o conceito de dados pessoais

Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016

Tratado sobre o funcionamento da União Europeia (versão consolidada)

Webgrafia

APDSI (2017) O tratamento de dados pessoais em Portugal. Breve Guia prático. Disponível em:

http://www.apdsi.pt/wpcontent/uploads/prev/Guia%20Pr%C3%A1tico_Vers%C3%A3o%20FINAL.pdf

Comissão nacional de proteção de dados (informações gerais), disponível em: https://www.cnpd.pt/

Conselho europeu (informações gerais). Disponível em:

https://www.consilium.europa.eu/pt/

CNPD (2017). 10 Medidas para preparar a aplicação do regulamento europeu de proteção de dados. Disponível em:

https://www.cnpd.pt/home/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf

Cordeiro, S. & Gouveia, L. (2018). Relatório Interno TRS 07/2018: Regulamento geral de proteção de dados (RGPD): o novo pesadelo nas empresas? Disponível em:

https://bdigital.ufp.pt/bitstream/10284/5953/1/RI_trs_07_2017.pdf

Ethics Advisory Group Report (2018). Disponível em:

https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

European data protection supervisor. Disponível em:

https://edps.europa.eu/

Grupo do artigo 29ª para a proteção de dados. Orientações sobre os encarregados da projeção de dados. (2016). Disponível em:

https://www.cnpd.pt/home/rgpd/docs/wp243rev01_pt.pdf

Hertzberg, E. (2018). What role can internal auditors play in GDPR compliance? Disponível em:
https://iapp.org/news/a/what-role-can-internal-auditors-play-in-gdpr-compliance/

Institute of internal auditors (IIA) (2019). GDPR: What? When? Why? Disponível em:

https://www.iia.org.uk/resources/auditing-business-functions/data-protection/gdpr-what-when-why/

IPAI (2017). Regulamento Geral de Proteção de Dados. Regulador e auditores: Parceria Estratégica? Disponível em:

https://www.ipai.pt/fotos/gca/cnpd_ipai_nov_2017_1511457275.pdf

Lambelho, A. & Mendes, J. (2019). X Congresso internacional de ciências jurídico-empresarias. O RGPD e o impacto nas organizações: 6 meses depois. Disponível em:

https://bibliotecadigital.ipb.pt/bitstream/10198/20369/1/Atas_CICJE_RGPD_Menores_RuteCouto.pdf

Machado, J. (2014). A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. Disponível em:

https://egov.ufsc.br/portal/conteudo/expans%C3%A3o-do-conceito-de-privacidade-e-evolu%C3%A7%C3%A3o-na-tecnologia-de-informa%C3%A7%C3%A3o-com-o-surgimento

Marques, J. (2017), Suporte de Regulamento Geral de Proteção de Dados: Regulador e auditores: Parceria Estratégica? Disponível em:

https://www.ipai.pt/fotos/gca/cnpd_ipai_nov_2017_1511457275.pdf

https://www.ipai.pt/fotos/gca/programa_conferencia_ipai_2017_0utubro_26_1509026264.pdf

Ordem dos contabilistas certificados (OCC) (2018). Manual de apoio à implementação do regulamento geral de proteção de dados (RGPD). Disponível em:

https://www.occ.pt/fotos/editor2/manualrgpd_maio2018.pdf

Referências bibliográficas. Disponível em:

https://apastyle.apa.org/

Silva, J. (2018). O encarregado de proteção de dados no regulamento geral de proteção de dados. Vida económica, Pág. 34. Disponível em:

https://www.occ.pt/fotos/editor2/ve_26janjpfs.pdf

Apêndice 1 – Questionário realizado

RGPD (Regulamento geral de proteção de dados): conhecimento e impacto nas organizações

O presente inquérito enquadra-se no âmbito da dissertação de mestrado "Regulamento geral de proteção de dados: conhecimento e impacto nas organizações, para conclusão do segundo ano do mestrado em auditoria no ISCAP.
Destina-se aos encarregados de proteção de dados, e também às pessoas que no âmbito da sua atividade profissional tratam dados pessoais, em empresas do PSI 20 .
Os dados fornecidos destinam-se única e exclusivamente ao estudo no âmbito da dissertação e em termos estatísticos, sendo garantida a confidencialidade dos mesmos.
Considere para todas as respostas a empresa para a qual trabalha.
Agradeço desde já a sua colaboração no preenchimento do questionário.
Qualquer dúvida, não hesite em contactar: flaviarsmachado@gmail.com

*Obrigatório

1. Sexo *

- ◯ Feminino
- ◯ Masculino

2. Idade *

- ◯ 25 - 35 anos
- ◯ 35 - 45 anos
- ◯ 45 - 55
- ◯ > 55 anos

3. Qual a função/departamento que ocupa atualmente? *

- ◯ Encarregado de proteção de dados
- ◯ Recursos humanos
- ◯ Auditoria interna
- ◯ Outra: _____

*

	Discordo	Nem concordo nem discordo	Concordo em parte	Concordo totalmente
4. Tenho conhecimento dos temas abordados pelo RGPD (Regulamento geral de proteção de dados)?	○	○	○	○
5. Considero que a empresa se encontrava preparada quando o RGPD passou a ser obrigatório, proporcionando os recursos necessários e adotando medidas adequadas. (Políticas, processos internos)	○	○	○	○
6. Considero que o impacto do regulamento na empresa foi minimizado, dado que existiu uma consciencialização geral sobre a privacidade e proteção de dados dentro da organização.	○	○	○	○
7. O tema tem sido "adiado" e não existe até então alterações significativas de processos, não sendo percebida muita preocupação e abertura para aplicação deste regulamento.	○	○	○	○
8. Considero que este regulamento alterou substancialmente a forma de trabalho, trazendo várias preocupações, procedimentos adicionais e alterando vários processos existentes.	○	○	○	○
9. A adoção de novas práticas á luz do RGPD trouxe melhores resultados ao nível de satisfação de clientes/funcionários/melhoramento de processos e menor utilização de recursos.	○	○	○	○

10. Tenho conhecimento que existe encarregado proteção de dados na empresa ou desempenho essa mesma função.	○	○	○	○
11. Considero a temática bastante complexa, e sinto necessidade de formação profissional ou informação de esclarecimento sobre o tema.	○	○	○	○
12. Considero que o encarregado de proteção de dados tem as competências profissionais necessárias e pertinentes para desempenhar as suas funções.	○	○	○	○
13. O trabalho realizado pelas auditorias de conformidade no âmbito do RGPD (externas) ajuda à clarificação de temas, fornece sugestões de melhoria e apoia na adoção de novos procedimentos.	○	○	○	○
14. A auditoria interna tem um papel ativo no apoio ao cumprimento do RGPD, assumindo papel preponderante na gestão de riscos e definição de controlos.	○	○	○	○