Universidade do Minho
Escola de Direito

João Juvenal Camacho Pereira

A Segurança da Privacidade da Informação e a Implementação do RGPD: o papel do EPD

julho de 2021

UMinho | 2021 João Juvenal Camacho Pereira **A Segurança da Privacidade da Informação e a Implementação do RGPD: o papel do EPD**

Universidade do Minho
Escola de Direito

João Juvenal Camacho Pereira

A Segurança da Privacidade da Informação e a Implementação do RGPD: o papel do EPD

Tese de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação do
Professor Doutor Francisco Andrade

e do
Professor Doutor Vítor Fonte

julho de 2021

Direitos de autor e condições de utilização do trabalho por terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos. Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho

Atribuição

CC BY

https://creativecommons.org/licenses/by/4.0/

Agradecimentos

Mais do que palavras de apreço, um louvor imenso aos meus pais. Juvenal Pereira, guerreiro e vencedor de todas as batalhas, lutador em prol dos filhos. Graça Pereira, persistente, positiva e paciente, lutadora em prol dos filhos.

Um agradecimento imenso à minha irmã Mara e companheiro, ao irmão Márcio e companheira, cúmplices desta conquista e que sempre mantiveram a proximidade, mesmo separados pelo Oceano Atlântico.

À justificação de todo o trajeto bem sucedido, companheira de todas as horas, a força de vencer todos os sacrifícios, à minha Sofia pelo respeito, dedicação e amor. À família do Norte, pelo acolher genuíno.

Aos meus amigos do Atlântico, o Ferraz, o Correia e o Vasconcelos. Aos meus amigos do Norte, o Lopes, o Aprígio e o Rodrigues.

Aos restantes familiares, amigos, equipa docente e orientadores que proporcionaram as melhores condições, não só para a dissertação, como no sucesso académico e profissional.

Declaração de Integridade

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Resumo

A Segurança da Privacidade da Informação e a Implementação do RGPD: o papel do EPD

A temática a dissertar é tripartida intuitivamente numa componente técnica fundada em padrões de boas práticas relativos à Informação, aos dados pessoais e à Privacidade (advindos das famílias de Normas ISO 27000 e 29000). Numa outra componente, desenvolve-se uma investigação jurídica acompanhada dos fundamentos históricos e preceitos do Regulamento Geral sobre a Proteção de Dados e da legislação nacional *data* protecionista. Conclusivamente, efetua-se uma análise elucidativa acerca do papel do Encarregado de Proteção de Dados, debruçada na fase de implementação e na fase de pós adequação.

Embora a objetivação da investigação seja de índole prática, afigurou-se relevante percorrer as noções teóricas básicas associadas a cada componente no sentido de elevar progressivamente o conhecimento, culminando na aplicabilidade prática específica. Para que sejam interiorizados os aspetos exigidos a um Sistema de Segurança de Informação sólido e as nuances que o tornam mais centrado para a Segurança da Informação Privada, optamos, portanto, por iniciar pela conceituação das propriedades bases da Segurança de Informação, pelos riscos e ameaças, *et cetera*. Da mesma forma, não seria plausível conhecer da atuação do Encarregado de Proteção de Dados, sem que antes venham a serem dominados os preceitos do Regulamento Geral, a origem histórico-social do Direito Fundamental a proteger e a posição que este sujeito ocupe na Relação Jurídica em causa.

Por forma a explorar a atuação prática que recai à equipa de profissionais de proteção de dados, percorreremos algumas das tarefas fulcrais, nomeadamente, as auditorias de conformidade, a Avaliação de Impacto da Proteção de Dados Pessoais e a comunicação da decorrência de violações de dados pessoais. A intuição da redação não se cingirá exclusivamente na conformidade da organização enquanto Pessoa Coletiva, mas antes na salvaguarda imprescindível dos direitos dos titulares de dados pessoais enquanto figura central determinante de todo trajeto histórico-normativo.

Palavras-chave: Dados pessoais, encarregado de proteção de dados, privacidade, sistema de gestão da segurança da informação.

Abstract

Information Privacy Security and GDPR Implementation: the role of DPO

The theme to be disserteted is intuitively tripartite in a technical component based on standards of good practices about information, personal data and privacy (respectively, from the ISO 27000 and 29000 families). In another component, a legal investigation is carried out about historical foundations, the precepts of the General Data Protection Regulation and the national data protectionist legislation. In conclusion, an explanatory analysis is carried out about the role of Data Protection Officer, focused on the implementation phase and the post adaptation phase of the legal precepts.

Although the objectification of the investigation has a pratical nature, it seemed relevant to go through the basic theoretical aspects associated with each component in order to progressively raise knowledge, culminating in specific pratical applicability. In order to internalize the aspects required for a solid Information Security System and the aspects that make it more focused on Private Information Security, we therefore chose to start by conceptualizing the basic properties of Information Security, the risks and threats associated, et cetera. In the same way, it would not be plausible to know about the performance of the Data Protection Officer, without first mastering the precepts of the General Regulation, the historical and social origin of the Fundamental Right to be protected and the position that this subject occupies in data relationship.

In order to explore the pratical role that must be performed to the team of data protection agents, we will go through some of the key tasks, such as compliance audits, the Data Protection Impact Assessments and the communication of personal data breaches. The intuition of writing spirit will not be restricted solely to the organization's compliance as a legal entity, but rather to the essential safeguarding of the rights belonging to personal data holders, as a central base of historical and data normative course.

***Key words**: Data Protection Officer, Information Security Management System, Personal data, Privacy.*

"Uma força perseguida
que na escolha do mais forte
faz com que a força da vida
seja maior do que a morte." [1].

[1] José Carlos Ary dos Santos, no poema "As Portas que Abril Abriu" recitado em 1975.

Índice

Índice de Figuras

Índice de Tabelas

Abreviaturas

Ac. – Acórdão

ACP – Autoridade de Controlo Principal

AIPD – Avaliação de Impacto sobre a Proteção de Dados

Al. – Alínea

Art. – Artigo

Arts – Artigos

BPMN – *Business Process Management Notation*

BTC – *Bitcoin*

CADA – Comissão de Acesso aos Documentos Administrativos

CdE – Conselho da Europa

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CE – Conselho Europeu

CEDH – Convenção Europeia dos Direitos do Homem

Cfr. – Conforme

CNPD – Comissão Nacional de Proteção de Dados

CNPDPI – Comissão Nacional de Proteção de Dados Pessoais Informatizados

CP – Código Penal

CPA – Código de Procedimento Administrativo

CPO – *Chief Privacy Officer*

CRP – Constituição da República Portuguesa

CSIC – Comité de Segurança da Informação e *Compliance*

CT – Código do Trabalho

DAMA – *Data Management*

DDoS – *Distributed Denial of Service*

DLP – *Data Loss Prevention*

DMBOK – *Data Management Body of Knowledge*

DMZ – *Demilitared zone*

DoS – *Denial of Service*

DPO – *Data Protection Officer*

EOA – Estatuto da Ordem dos Advogados

EPD – Encarregado de Proteção de Dados

GDPR – *General Data Protection Regulation*

GT 29 – Grupo de Trabalho do artigo. 29º para a Proteção de Dados (da Diretiva 95/46/CE)

IDS – *Intrusion Detection System*

IoT – *Internet of Things*

IP – *Internet Protocol*

IPS – *Intrusion Prevention System*

IRS – Imposto sobre o Rendimento de Pessoas Singulares

ISO – *International Organization for Standardization*

LADA – Lei de Acesso aos Documentos Administrativos

LNE – Lei Nacional de Execução (do Regulamento Geral sobre a Proteção de Dados): Lei n.º 58/2019, de 8 de agosto.

N.º – Número

Ob. Cit. – Obra Citada

Pág. – Página

Págs. – Páginas

DPIA – *Data Protection Impact Assessment*

PME – Pequenas e Médias Empresas

PSI – Política de Segurança de Informação

RGPD – Regulamento Geral sobre a Proteção de Dados

SGPI – Sistema de Gestão da Privacidade da Informação

SGSI – Sistema de Gestão de Segurança da Informação

SS – Seguintes

UE – União Europeia

VPN – *Virtual Private Network*

WAF – *Web Application Firewall*

WP – (*Article 29 Data Protection) Working Party*

Introdução

O *desideratum* da escolha de temáticas de Proteção de Dados Pessoais conjugadas com Sistemas de Segurança da Informação tem a sua génese na conclusão do primeiro ano de mestrado em Direito e Informática pela Universidade do Minho. Os preceitos legais outrora conhecidos de forma genérica deixaram em aberto a forma como seriam postas em prática as exigências que se retiram do Regulamento Geral sobre a Proteção de Dados[2]. Mais do que verificar a sua índole prática, fortificou-se a curiosidade em dissertar sobre o impacto que resulta do disposto comunitário (entenda-se, com entrada em vigor, de forma simultânea, em todos os Estados Membros da União Europeia, inclusive o Reino Unido que deteve a aplicabilidade direta até à aprovação do *Brexit*[3]) sobre o quotidiano dos titulares dos dados pessoais e das entidades encarregues de garantir a salvaguarda do direito à proteção de dados pessoais (privadas, organismos públicos e, em certas circunstâncias, pessoas singulares).

Na prossecução da objetividade em adquirir conhecimentos específicos sobre esta matéria, implicará dissertar preliminarmente sobre os sistemas que garantem a segurança da informação pessoal na sua essência e o enquadramento jurídico que se retira do Regulamento para elucidar-nos acerca da Proteção de Dados Pessoais em termos gerais. Só após a familiarização sobre estes assuntos é que se dissertará sobre do papel do Encarregado de Proteção de Dados para alcançar a concretização dos preceitos legais, num nível mais circunscrito.

---

[2] Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (doravante, abreviadamente designado por RGPD).

[3] Enquanto países externos à União Europeia, toda a transferência de dados para os países pertencentes ao Reino Unido, careceriam de legitimidade já que passam a estar enquadrados nos parâmetros de transferências internacionais (cfr. artigos 44.º e ss do RGPD). O certo é que, em consonância com a aplicabilidade do Regulamento Geral sobre a Proteção de Dados que outrora decorreu, a decisão de adequação a ser emanada pela Comissão Europeia estaria na iminência de ocorrer pela similaridade do quadro legislativo data protecionista. A comissão Europeia não garantiu, atempadamente, a aprovação do "acordo de fluxo de dados" com o regime britânico relativo à proteção de dados, antes do período de transição do Brexit terminar – em janeiro de 2021. Desde então (e enquanto solução temporária de 6 meses), o Reino Unido permaneceu num quadro de transferência de dados da UE até que fosse definitivamente comprovado o grau de equivalência data protecionista. A 28 de Junho de 2021, a decisão de adequação (em matéria de RGPD e, por outro lado, em matéria da Diretiva (UE) 2016/680) para o livre fluxo de dados pessoais para o Reino Unido foram adotadas pela Comissão Europeia, decisão fulcral para a correta implementação do Acordo de Comércio e Cooperação EU-UK (cfr. decisão consultável em https://ec.europa.eu/commission/presscorner/detail/pt/IP_21_3183?fbclid=IwAR1ArbxGgy0QLXcJGjPiZIyk4k6XXoG9NRnvsxWyW2P9_ABtetwg5bxdRPI). Um dos elementos chave para a identificação de tal equivalência seguiu pelo facto do quadro legislativo ter por base ainda o RGPD e demais legislação comunitária associada. No entanto, e reconhecendo que as decisões de adequação são automaticamente expiradas passados 4 anos, e renovadas se se mantiver a equivalência (daí a designação de "*sunset* clause"), caso haja alteração da *ratio* da estrutura legal sobre a proteção de dados pessoais, poderá implicar na retirada ou não renovação destas decisões de adequação surgir – cfr. n.º9 do artigo 45.º do RGPD.

Para além do fator momentâneo que sublinha o interesse pelo estudo em causa, já que a aplicabilidade do Regulamento UE 2016/679 teve a sua entrada em vigor a 25 de maio de 2018, a nova abordagem rigorosa que dele se retira (acerca de questões relacionadas com a segurança e a privacidade dos dados pessoais) faz repensar o valor que um simples dado pessoal preenche para os sujeitos titulares, para o tecido empresarial ou governamental, para a privacidade, para o comércio e para a segurança.

O Diretor Executivo da *The Futures Agency* descreve, no *Business Transformation Summit* de 2017 que "o novo petróleo são os dados"[4]. Desde o início do século, com a ascensão das redes sociais, com a impulsão do uso das vias cibernéticas para efetuar atividades sociais ou por comodidades, além das recentes evoluções no âmbito da Inteligência Artificial e de dispositivos interconectados (Internet das Coisas), implicaram uma reformulação na legislação comunitária, por forma a que se reforçasse a salvaguarda pela proteção dos dados pessoais, dependente das vontades e valores éticos de cada empresa multinacional. Todavia, a carência de um sistema de segurança e o valor dos dados, mesmo aqueles cujo caráter não seja pessoal, não é novidade deste século. Se imaginarmos, na distante era da pirataria, a interceção de uma fragata detentora de documentações que indicassem as rotas mercantis programadas, isto é, detentora de um arquivo (ou, digamos, base de dados) militarmente protegido, quando caísse em mãos alheias poderia colocar em causa a segurança e a riqueza de uma nação.

Embora a privacidade, nos seus termos gerais, já esteja preenchida de proteção jurídica desde a Convenção Europeia dos Direitos do Homem, nos termos do artigo 8.º, a informação pessoal tornou-se um problema de privacidade à escala mundial com o culminar da ascensão científico-tecnológica no término do século XX, ao ponto de suscitar a sua regulação com maior rigor, fundamento que originou a criação do RGPD[5]. Até então, o desvalor associado aos dados pessoais parece estar intrínseco aos próprios titulares. Eram partes pouco participativas, menos informadas acerca do mundo tecnológico, e desinteressadas pelo que dele poderia impactar na sua vida privada.

Citando o historiador e escritor israelita YUVAL HARARI (2018) "No apogeu do imperialismo europeu, os conquistadores e os negociantes adquiriam ilhas e países inteiros em troca de

[4] Artigo de JE editors e Cegoc *in* Jornal Económico, 2017, disponível em: https://jornaleconomico.sapo.pt/noticias/o-novo-petroleo-sao-os-dados-229587 (consultável em julho 2021).
[5] Cfr. LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E* para as organizações?, FCA, 2018, pág. XV.

contas de vidro. No século XXI, os dados pessoais são provavelmente o bem mais valioso de que os seres humanos dispõem e estamos a oferecê-los aos gigantes tecnológicos em troca de *e-mail* e vídeos engraçados de gatinhos"[6].

Estruturalmente, a divisão tripartida da dissertação seguirá a formação de três capítulos. No capítulo 1º adota-se uma perspetiva organizacional, expondo os mecanismos e sistemas que os detentores de responsabilidades na Segurança da Informação devem preencher. O desenvolver do primeiro capítulo segue fielmente os tópicos do guia de preparação para a certificação dos Fundamentos Básicos de Segurança de Informação, baseados na ISO/IEC 27001 e 27002, exposto no site oficial da EXIN[7] e tem auxílio do Curso Preparatório para a certificação criado pelo Professor Cláudio Dodt na plataforma Udemy, sem prescindir de consulta bibliográfica complementar. Serão expostas as temáticas de Propriedades basilares da Segurança da Informação, de Políticas de Segurança da Informação, de Gestão de Riscos e de Incidentes e as medidas de segurança (não apenas técnicas e organizacionais, mas também as medidas de segurança físicas já que o Regulamento protege dados pessoais na sua amplitude e não, exclusivamente, dados pessoais armazenados em formato digital, atendendo ao seu considerando 15.º). Será finalizado com elucidação da norma ISO 27701, sendo uma padronização específica da Segurança da Informação Privada.

De seguida, no 2º Capítulo analisar-se-á os preceitos normativos *data* protecionistas no âmbito comunitário e no âmbito nacional, nomeadamente os dados pessoais que se consideram alvo de proteção, o respetivo tratamento (licito, leal e transparente), os sujeitos que ocupam posições distintas na relação em causa e, abrindo caminho para o último capítulo, as especificidades da figura do Encarregado de Proteção de Dados, sublinhando o acompanhamento das disposições normativas do Regulamento Geral sobre a Proteção de Dados, da Lei n.º 58/2019 de 8 de agosto e as orientações que se afigurem imprescindíveis do Grupo de Trabalho do Artigo 29º[8] da Diretiva 95/46/CE. A sua redação segue o suporte bibliográfico relevante nesta matéria e o auxílio da formação para a certificação CIPP/E da IAPP, fornecido pela *Breach Consulting* enquanto parceiro oficial.

[6] *Apud* YUVAL HARARI, Homo Deus: História Breve do Amanhã, 2017.
[7] Guia de temáticas de 2020/2021 consultável em https://www.exin.com/br-pt/certificacoes/#certifications/information-security-foundation-based-iso-iec-27001-exam
[8] Substituído pelo atual Comité Europeia de Proteção de Dados Pessoais, segundo o Considerando 139 do RGPD.

Finalmente, o terceiro e último capítulo da dissertação incorpora a aplicabilidade prática do Regulamento (e o papel a desempenhar pelo EPD), à qual implica distinguir o momento de implementação primária do RGPD, isto é, a implementação em uma organização que inicie a sua atividade ou que já tenha iniciado, mas não tenha efetuado os procedimentos prévios necessários para estar em conformidade. Por outro momento, dada a implementação como concluída, haverá um conjunto de processos, revisões e avaliações[9] a ter em conta na fase de pós-implementação para que a organização mantenha a adequação necessária do estado de *compliance*. Este faseamento de conformidade, além de seguir a bibliografia imprescindível, auxilia-se do curso breve de "RGPD para implementadores na Administração Pública" disponibilizado na plataforma da "NAU – Sempre a Aprender", em parceria com a "INA – Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas"[10].

De modo conclusivo, serão enunciadas as principais ideais, conclusões e alguns aspetos que nos parecem ficar por clarificar.

[9] Com auxílio das Normas ISO 29100 (Técnicas de Segurança), 29134 (AIPD) e 29151 (Código de Práticas para a Proteção de Dados Pessoais)
[10] Consultável em Julho de 2021, Disponível em: www.nau.edu.pt/curso/rgpd-para-implementadores-na-administracao-publica/

CAPÍTULO I – A Segurança da Informação e a Privacidade

1. Informação e Segurança

1.1. Conceituação

A Informação é a correlação de dados contextualizados. O dado por si só não possui contextualização, é uma partícula mínima, isolada, sem elo. A passagem para a informação dá-se ao acrescentar contexto temporal, espacial ou com personificação atribuída. Se agregarmos um entendimento adicional aos dados contextualizados (por exemplo, sobre a sua utilidade) alcançamos o conhecimento. Na atualidade, qualquer operação relacionada com estes conceitos não se distingue se provirá da atuação humana ou por meios automatizados, mas ao acrescentarmos valor à informação atingimos o patamar da sabedoria, **alcançável exclusivamente pela mente humana**[11].

No seio organizacional, a informação surge incorporada nos processos de negócio. Atualmente, é considerada fator de produção, alargando a tríade de produção tradicional - Capital, Trabalho e Matéria Prima – ao ponto de ser reconhecida enquanto produto final, imprescindível para a operacionalidade e rentabilidade de certas organizações. Existem empresas que têm na Informação a sua base dos processos negociais, como é o caso da *UBER* que, pese embora a sua atividade dependa da existência de veículos quer para o transporte de passageiros, como para a entrega de mercadorias, sendo esse o seu âmbito empresarial, ela não possui carros enquanto propriedade da empresa. Tem a informação como a base negocial, mais concretamente, a localização dos passageiros ou moradas de recolha e de entrega, o interesse em usufruir da prestação de serviços em causa e a conexão com os motoristas por mecanismos de geolocalização e contactos pessoais. O mesmo ocorre nas grandes empresas que apresentam um catálogo organizado de alojamento local na esfera do *e-commerce* em que recebem informação de interesse de hospedagem por parte da clientela e transmite a informação de quem possui imóveis disponíveis para alojar, mesmo que não

[11] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 2, ponto 3 e 4, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

tenha em sua posse qualquer imóvel — tomemos como exemplo a *Airbnb*. Nestes parâmetros empresariais, há uma dependência em conhecer a informação para que decorra a prestação de serviço. Não depende, portanto, da recolha de dados por si só, mas sim da recolha de dados processados e contextualizados[12].

É claro que, nestas circunstâncias o valor da informação será mais acrescido do que em empresas tradicionais (que tenham a sua atividade centrada no comércio de retalho, por exemplo) embora haja valor da informação ainda que mais reduzido, delimitado de acordo com a tipologia, finalidade e estrutura da organização. O valor da informação é atribuído pelo utilizador, o destinatário da informação, já que a sua caraterização é que determina qual a informação, para si, relevante. Especifiquemos na prática refletindo acerca dos serviços da *UBER*: o cliente atribui valor acrescido à informação que tenha relação aproximada com o espaço que lhe circunda. À partida, não importa informações de motoristas disponíveis na França, se a sua localização indica estar em Portugal. Portanto, voltamos, então, a destacar os dados contextualizados. A ISO 27002 descreve na cláusula 0.1 – Propósito e Contexto – que "o valor da informação vai além das palavras, números e imagens escritas: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis de informação".

Tipologicamente, a informação não parte apenas de formatação digital. Quer esteja armazenada por meios físicos ou por meios digitais (num sistema informático ou em trânsito pela rede), carecerá de proteção física, técnica e administrativa já que, como veremos adiante, de nada vale a uma empresa ser portadora de mecanismos de proteção digital aperfeiçoados se as credenciais de acesso ou documentos confidenciais estiverem expostos ao público em geral e desprotegidos de um perímetro de segurança, por forma a estarem disponibilizados a quem não deva acedê-los. Em todo o **ciclo vital**[13] associado à informação que passa pela criação, armazenamento ou processamento (coleta de dados para agregar aos contextos), transporte, atualização e apagamento, devem ser considerados mecanismos de segurança. Ainda que os critérios de proteção dependam sempre do valor negocial atribuído à informação, a existência dum Sistema de Segurança da Informação confiável exige o planeamento de proteção para todos os ciclos vitais — a denominada *Security by Design* que

[12] No caso da *Airbnb,* são dados contextualizados a existência do prédio imóvel com referência de morada, de tipologia, do preçário específico consoante época sazonal ou nº de pessoas a usufruir da habitação, em que datas apresenta tal disponibilidade, entre outros dados que individualizam aquela oferta.
[13] ISO 27002, cláusula 0.5 – Considerações do Ciclo Vital – pág. Vii.

o Regulamento Geral sobre a Proteção de Dados privilegia — até mesmo na sua destruição, sob pena de levar à posse de pessoa não autorizada[14].

Partindo da temática em análise, reporta ressalvar uma distinção entre os termos de Segurança de Dados e Privacidade de Dados, sendo que o primeiro implica a existência de mecanismos de proteção para com ataques, incidentes de Segurança de Informação, invasões de sistemas, et cetera. Já o segundo está concentrado nos direitos individuais entranhados, enquanto finalidade da Segurança da Informação, por exemplo, a quebra da confidencialidade viola a privacidade da informação em si, ainda que meta em causa os mecanismos ponderados para essa proteção. Então, a Segurança da Informação visa proteger a Privacidade da Informação, entre outras prioridades, vejamos adiante.

1.2. Propriedades Base da Segurança da Informação

Um Sistema seguro implica a existência de mecanismos planeados e implementados para a proteção de determinadas propriedades[15].

No que concerne a um Sistema de Informação, os mecanismos desenhados são projetados para garantir a plenitude das propriedades fundamentais da informação. Sublinhando a indicação de SIMÃO DE SANT'ANA e VITORINO GOUVEIA[16], "A norma ISO 27001 é um modelo de referência para a implementação de um SGSI numa organização, independentemente da sua dimensão, setor e âmbito de aplicação". Se formos ao encontro da família de normas ISO 27000, em concreto na ISO 27001, as bases projetadas para a implementação de um SGSI são, essencialmente, a Confidencialidade, a Integridade e a Disponibilidade[17].

A **Confidencialidade** é reconhecida enquanto garante do acesso autorizado, isto é, a proteção da informação (estática ou em trânsito pela rede) perante divulgações ou interceções acessíveis por partes não autorizadas. Embora os controlos de segurança venham a ser elucidados detalhadamente mais adiante, podemos já considerar que esta propriedade

[14] Cfr. LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E* para as organizações?, FCA, 2018, págs. 66 a 68.
[15] Cfr. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, pág. 48.
[16] *Cfr*. SIMÃO DE SANT'ANA e VITORINO GOUVEIA, *in* "O RGPD e os Recursos Humanos – Guia Prático para a Conformidade", Almedina, 2021, pág. 48.
[17] ISO 27001, na cláusula 0.1 – Introdução, Geral – "The information security management system preserves the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed" – pág. V.

é assegurada por mecanismos de controlo de acesso, por segregação de funções (conceder acesso específico consoante funções a desempenhar pelo colaborador) e por algoritmos de cifragem que garantem a transformação da informação real em informação ininteligível, mesmo que intercetada por quem não deva ter acesso. Na prática a sua violação surge, usualmente, pelo acesso a documentação empresarial por parte de colaboradores não autorizados que intercetam a informação no momento da impressão dos documentos ou por funcionários que se encontram em fases de despedimento, além do acesso ou divulgação de planos estratégicos para a concorrência.

Quanto à **integridade** da informação implica que permaneça completa, exata e verdadeira, sem que sofra alterações intencionais ou acidentais desde a sua elaboração original. Nesta, o controlo de acesso e as técnicas de criptografia possibilitam, de igual modo, a verificação da propriedade através de códigos de integridade cifrados por uma chave secreta e por funções de *hashing* (a alteração do conteúdo de uma mensagem será facilmente reconhecida). Nas circunstâncias de erros de integridade, pode a organização estar sujeita à impossibilidade de restauro de cópias de segurança (o denominado *backup*) que, cumulativamente, afetará outras propriedades de segurança de informação, pelo que é aconselhado o seu controlo por mecanismos de monitorização e auditorias regulares.

Para garantir a **disponibilidade**, importa que a informação permaneça consultável, acessível e utilizável, à luz do que se considere uma utilização expectável. Em prática, está dependente de serviços disponíveis em hiperligações, plataformas de subscrição ou outras, o que exige o controlo da interoperabilidade e do servidor que disponibilize a informação. Em formato impresso, o desaparecimento dum arquivo significa uma quebra da disponibilidade. É posta em causa, por exemplo, através dum ataque de negação de serviços (DoS – *Denial of Service*[18]) que torne um dispositivo computacional ou um recurso de rede indisponível. Quanto aos controlos adequados para garantir tal propriedade, de um modo genérico, importa as regulares cópias de segurança, ter implementado um plano de continuidade e recuperação em caso de catástrofes, além de processos de recuperação adequados, pelo que

[18] Analogamente, existem ataques DDoS – *Distributed Denial of Service* – em que o ataque ao tráfego de entrada é proveniente de diversas fontes, condicionando o acesso legítimo de clientes. Num contexto físico, temos como exemplo o bloqueio da entrada da loja comercial. A interrupção das operações é a consequência direta destes ataques.

estará muito dependente de medidas organizacionais, essencialmente de políticas de segurança[19].

A preservação das propriedades da informação, conjuntamente com fatores essenciais da informação[20], entre eles, Pessoas, Processos e Tecnologia[21], fomenta, nos termos da ISO 27001, a Segurança da Informação[22] e o combate adequado aos riscos associados, enquanto meio para garantir os objetivos negociais, isto é, para que execute os processos negociais da forma mais adequada possível perante as avultadas ameaças e riscos, o que implica a sua conformidade com os tramites legais. Existem propriedades derivadas desta tríade fulcral, nomeadamente a autenticidade – veracidade da alegação de origem (autoria) — responsabilidade (derivada da expressão inglesa *"accountability"*) e não repúdio enquanto forma de atribuir uso à informação por parte da empresa[23].

Ainda assim, uma boa gestão de Segurança de Informação não significa a inexistência total de incidentes de segurança, mas através de controles adequados garantimos a **minimização das consequências provenientes de incidentes**, consoante os padrões de segurança aconselháveis. Um nível inviolável de segurança de informação é puramente teórico, mas o planeamento, a implementação e a revisão de mecanismos de segurança aconselhados segundo orientações internacionais fazem a diferença. A própria legislação comunitária[24] reconhece que a atuação adequada será aspeto de reflexão nas fases de fiscalização e a aplicação de sanções por parte da Autoridade de Controlo. O certo é que as medidas adequadas, entre as quais as medidas técnicas e organizacionais por referência ao artigo 32.º RGPD, estão associadas à análise contextual da empresa[25], aos riscos reais concretos que a ela acarretam, ao que está realmente vulnerável, pelo que não se espera uma

[19] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 2, ponto 6, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

[20] Um sistema seguro exige um equilíbrio entre os seus fatores essenciais, porque para retirar utilidade de uma tecnologia modernizada é necessária a sua utilização adequada por parte das Pessoas. Mesmo que uma organização elabore processos úteis e esteja dotada de tecnologias adequadas, podem surgir brechas de vulnerabilidades que ponham em causa as propriedades se os seus colaboradores não seguirem as Políticas de Segurança, nem detenham a formação básica para ao conhecimento da sua utilização.

[21] ISO 27001- cláusula 5.1, alínea b) para os processos – pág. 2; cláusula 5.1, alínea c) e cláusula 7.1 para as pessoas e tecnologias – págs. 2 e 5.

[22] Mais do que segurança digital, a segurança da informação visa a sua proteção em qualquer formato, seja em meios eletrónicos, impressos ou até a manifestada em diálogo entre as partes interessadas. – ISO 27002, na cláusula 0.2 – Introdução, A prática e o contexto – "Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations)." – pág. vi

[23] Cfr. JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, págs. 2 e 3.

[24] Essencialmente, no n.º2 do artigo 83.º do RGPD.

[25] ISO 27001 – cláusula 4 – passa por compreender o contexto da organização, por determinação dos problemas externas e internos; as necessidades e expetativas das partes interessadas ao propósito; determinar o objeto do SGSI; implementar, manter estável e promover continuamente um SGSI em concordância com os padrões internacionais aconselhados nesta Norma.

aplicação idêntica *stricto sensu* dos mecanismos de segurança entre organizações diferenciadas quanto ao seu âmbito, às suas operacionalidades, às ameaças e riscos que as individualizam[26].

2. Riscos e Ameaças

2.1. Terminologia e Tipificação das Ameaças

> *"Os ativos estão sujeitos a ameaças deliberadas e acidentais, enquanto os processos, sistemas, redes e pessoas relacionados têm vulnerabilidades inerentes" ISO 27002* [27].

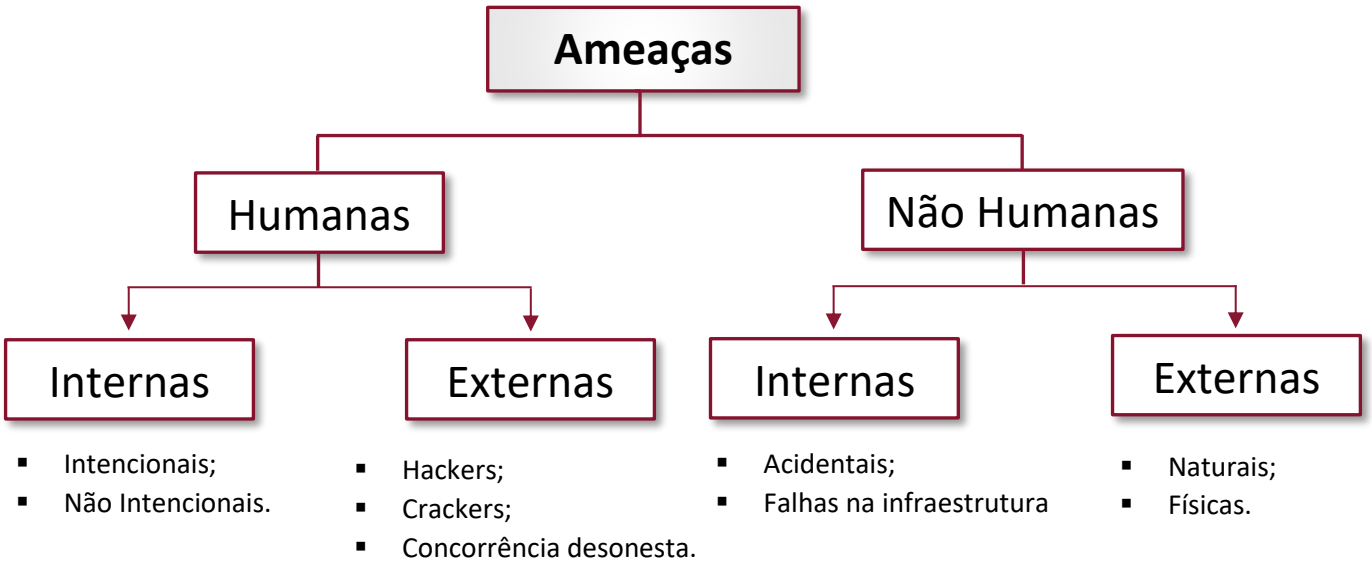
Partindo da nomenclatura, uma **ameaça** é a potencial origem dum incidente indesejável que possa afetar pessoas, processos e tecnologias, enquanto que um **risco** reside na combinação de consequências oriundas dum evento e da probabilidade de surgir tal ocorrência, ou seja, na incerteza de garantir o alcance objetivo através dos controlos e medidas de segurança que somos portadores. No caso da Segurança da Informação, os objetivos de proteção da confidencialidade, da integridade e da disponibilidade consoante as orientações da ISO 27001.

O risco na Segurança da Informação parte do potencial das ameaças explorarem as vulnerabilidades da informação e que, nesse contexto, venham a causar danos à organização. São conceitos cronologicamente relacionados. Mas se as ameaças não encontrarem uma vulnerabilidade que possam explorar, isto é, uma fragilidade de segurança num ativo de informação, elas não vão afetar a organização e é justamente neste contexto que relevam os mecanismos de segurança aplicados, enquanto meios de impedimento para que suscite exploração de vulnerabilidade, deixando o risco num nível aceitável já que a total inexistência do risco é humanamente impossível[28].

[26] Exemplo de aplicação diferenciada consoante o contexto organizacional parte da Cláusula 7.5.1, Nota e alíneas 1), 2) e 3), da ISO 27001, pág.6.
[27] Cláusula 0.1 – Propósito e Contexto – pág. Vi.
[28] ISO 27002, cláusula 0.1 – Propósito e Contexto – "*Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present.*" – pág. Vi, 4º parágrafo.

Tipologicamente há uma distinção entre as ameaças à segurança de sistemas e comunicações que provenham de uma atuação ou omissão humana e as não humanas, ambas com subdivisão de ameaças com origem interna ou externa, como se apresentam simplificadamente retratadas na Figura 1 *infra*.

Figura 1 - Tipologia de Ameaças



Nas ameaças humanas internas aos serviços ou recursos a proteger, surgem com caráter intencional, nomeadamente com atuação maliciosa e propositada por parte de algum colaborador, ou por erro não intencional, por exemplo, quando colaboradores colocam dados confidenciais numa esfera acessível ao público em geral, mas fá-lo por falta de preparação para utilizar de forma adequada a tecnologia ou por atuação negligente — "considera-se interna qualquer entidade autorizada de forma aparentemente legítima"[29]. De origem externa à entidade ocorrem as ameaças com tendencial foco de proteção, que influenciam a camuflagem do perigo inerente a outras ameaças. Por advir de entidades externas e sem autorização de acesso, são, na sua maioria, mais intrusivas e, consequentemente, mais detetáveis pelos administradores. São ameaças provenientes de agentes que não fazem parte da organização, sejam *crackers* (enquanto ciber criminosos com intuito de atuar ilicitamente), *hackers* (com fundamento em descobrir uma vulnerabilidade para exigir a sua ratificação ou

[29] Cfr. JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, págs. 3 e 4.

por intermédio de testes de intrusão autorizados pela própria entidade alvo) ou meros concorrentes desonestos que queiram aceder, por exemplo, a informação confidencial como o caso de segredos comerciais.

Nas ameaças de origem não humana podem advir da esfera **interna** à organização por possíveis destruições acidentais do equipamento ou arquivo ou por falhas na infraestrutura física, quando haja deterioração e danificação do estabelecimento ou defeitos do equipamento interno, falhas na rede elétrica ou erros de software ao ponto de colocar em causa a segurança da informação. As ameaças no âmbito **externo** à organização, estarão dependentes do contexto espacial que a entidade se localize ou armazene os seus equipamentos. São com causas naturais (catástrofes de inundações, tempestades, etc) ou físicas como por exemplo uma explosão, poluição ou contacto com água.

As ameaças são a possibilidade dum evento causar impactos nefastos, portanto, a possível origem dos danos. Distinguem-se os danos **diretos** quando advém prejuízo diretos devido à ameaça concretizada, dos **indiretos** quando sejam a consequência após o dano direto concretizado. Na prática, supondo que em caso de catástrofe o servidor do sistema é destruído, mas o servidor de *backup* não tenha sido afetado, ainda que haja uma desatualização das cópias de segurança de alguns dias. Neste caso, a destruição do equipamento e a perda de informação são danos diretos, mas podemos perspetivar como indiretos os custos para a recuperação de dados sem cópias de segurança, a indisponibilidade do sistema, perda de clientela e reputação ou até coimas associadas. Assim sendo, os danos indiretos serão as consequências após a catástrofe.

2.2. Gestão dos Riscos[30]

"Um SGSI tão específico quanto o proposto na ISO/IEC 27001, adota uma visão holística e coordenada dos riscos de segurança da informação da organização, para implementar um conjunto abrangente de controles de segurança da informação sob a estrutura geral de um sistema de gestão coerente" ISO 27002[31].

Tem a sua génese na **Política Geral de Segurança de Informação**[32] elaborada no enquadramento prático de cada organização, na qual se define como será encarado o risco para que ele se torne aceitável.

Existem três parâmetros a percorrer na gestão de riscos. O ponto de partida é a análise de riscos[33] para entender que riscos afetam em concreto a organização, com determinação de riscos reais contextualizados. Está intrínseca a tarefa de identificação da natureza e nível dos riscos, preenchida através do cálculo da probabilidade e do impacto representado por escalas numéricas (se optar por uma análise quantitativa, tendo por base modelos matemáticas e dados fatuais. É mais exata, mas exige uma análise mais trabalhosa e com reconhecimento aprofundado da situação) ou por escalas simplificadas e não numéricas (de análise qualitativa baseada em perceções das partes envolvidas). Mesmo numa análise

[30] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 3, ponto 7 a 11, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

[31] Cláusula 0.1 – Propósito e Contexto – pág. Vi, 5º parágrafo.

[32] Declaração formal da direção da organização que define os processos e objetivos da Segurança de Informação, contextualizado com a tipologia de empresa. – ISO 27001, cláusula 5.2 específica da PSI (pág. 2) e cláusula 6.2 quanto aos objetivos da segurança de informação (pág. 5) - Esta orientação, com apoio geral da direção, é o ativo estratégico central da Segurança de Informação para que se possa garantir o seu cumprimento. A eficiência da Política de Segurança de Informação só é garantida quando esta esteja alinhada às estratégias específicas da organização, aos seus regulamentos, contratos em vigor e legislação aplicável, mas, sobretudo, aos perfis de ameaças habituais que tende a enfrentar (aplicação organizacional específica para aderência à realidade prática). Ademais, importa a sua eficácia ao nível operacional, com as instruções e guias de trabalho transmitidos aos respetivos funcionários de modo suficiente para fomentar a consciencialização e execução eficiente, colocando a Segurança de Informação na prática, justamente porque através da PSI transmitimos a autorização formalizada para implementar as medidas de segurança necessárias. Deve ser perspetivada tanto para aspetos negociais como para aspetos de ciber segurança (TI), publicada adequadamente com vista à correta divulgação para as partes relacionadas, ser revista periodicamente e apoiada por outras medidas específicas (*infra* elucidadas). Em suma, trata-se da contextualização e propósito do Sistema de Gestão de Segurança da Informação da entidade na qual são indicadas, por diretrizes, a gestão dos riscos a percorrer, a responsabilidade, sanções e processos disciplinares correspondentemente imputados, caso não sejam acatadas essas orientações, entre outras orientações – PSI tem fundamento em boas práticas e normas, com intuito de estabelecer, implementar, monitorizar e aperfeiçoar a segurança da informação e é a 1ª medida estratégico organizacional num Sistema de Gestão e Segurança de Informação.
Para estabelecer garantias de comportamento seguro e adequado no que compete aos colaboradores, importa incluir alguns aspetos da PSI no próprio código de conduta (outra componente documental da organização da empresa), desde que não indique aspetos que comprometam as medidas de segurança. Pode até deixar explícito a existência de consequências se porventura forem praticados comportamentos contrários ao estipulado nos princípios da empresa.

[33] ISO 27001 – cláusula 6.1.2 págs. 3 e 4.

quantitativa, de modelo estatístico-valorativo bem definido, haverá sempre um determinado nível de incerteza. A análise usualmente executada é a qualitativa (Exemplificada na Tabela 1) na qual pesa sobretudo o nível de experiência do analista, com auxílio de listas de verificação (as denominadas *checklists*) e da técnica de *brainstorming*[34]. O aconselhável será a elaboração de uma análise qualitativa para que sirva como suporte da análise quantitativa, destacada pela exatidão.

Tabela 1 - Análise Qualitativa dos Riscos (Adaptada de Cláudio Dodt *et alia*, 2018).

		Impacto		
		Baixo	Médio	Alto
Probabilidad	Baixa	Baixo Risco	Baixo Risco	Médio Risco
	Média	Baixo Risco	Médio Risco	Alto Risco
	Alta	Médio Risco	Alto Risco	Alto Risco

Numa 2ª fase, decorre o tratamento dos riscos[35] onde é feita a seleção das medidas de segurança apropriadas para cada circunstância, alinhada aos recursos disponíveis, ao valor específico da informação que careça de proteção e a determinados fatores externos subordinados a cumprimentos contratuais e legislativas. A forma como o risco é tratado depende da estratégia de risco que se pretende encaminhar, seja com intuito de reduzir, evitar, transferir ou até aceitar o risco. Para exemplificar as diferentes estratégias para encarar o risco, vejamos uma circunstância em que o *data center* se encontra numa localização onde haja alta probabilidade de incêndio, por indicações de estudos estatísticos. Caso a estratégia passe pela redução do risco, bastaria um sistema de deteção e combate a incêndio, mas se for necessário evitar o risco então poderia os dados serem migrados para a *Cloud*. A contratação

[34] Técnica que privilegia o ambiente informal e descontraído, com participação de vários membros da organização, como meio para resolução do problema (neste caso, análise dos riscos existentes), com quebra de suposições incorretas, dotada duma vasta gama de soluções criativas, fruto da experiência diversificada entre os vários membros participantes. É a técnica ideal para perspetivarmos os riscos, já que conta com perspetivas diferentes e não com apenas um analista que elabore um processo estruturado e analítico. Disponível em: https://www.mindtools.com/brainstm.html (consultável a julho de 2021).

[35] ISO 27001 – cláusula 6.1.3.

de seguro contra todos os riscos estaria associada à estratégia de transferir o risco para outra entidade, embora ele se mantenha ativo. Ainda que seja considerado aceitável ao não comprometer as operações da organização, é fulcral efetuar o registo formal de que o risco foi aceite e o mesmo se aplica no caso de riscos residuais (os que sobrevivem à aplicação das medidas de segurança).

Tanto a análise dos riscos como o tratamento dos mesmos, devem estar alinhados com as orientações da ISO 31000, enquanto norma específica para a Gestão de Riscos.

Na fase conclusiva da gestão de riscos, há a implementação dos controlos de segurança[36] selecionados na fase anterior, com o intuito de modificar o risco para o nível aceitável[37]. A vasta gama de medidas de segurança diverge em tipificação consoante o momento para o qual têm a sua motivação[38]. Distinguem-se:

- **Medidas com caráter de dissuasão**, aplicadas perante uma ameaça antes de ser tornar um incidente, antes de explorar uma vulnerabilidade, dificultando a sua concretização. São medidas projetadas para prevenir a ocorrência do incidente;

- **Medidas com foco na deteção**, impostas quando o incidente já esteja em curso, **e na repressão** para aniquilação do incidente, antes de gerar qualquer impacto. São utilizadas num espaço temporal em que há exploração efetiva do incidente, com os objetivos de identificar a ocorrência indesejada e, a partir daí, atuar no campo da amortização dos seus efeitos.

- **Medidas para a correção**, surgem na situação de pós impacto, quando seja transformado em dano, por exemplo, quando sejam apagados acidentalmente os dados, a medida de correção do impacto seria o restauro através da cópia de segurança.

- **Medidas com caráter de avaliação**, decorrem na fase da recuperação e servem como comando de investigação para reconhecer o que falhou, o que precisa ser melhorado e corrigido.

[36] ISO 27001 Anexo A, com especificações detalhadas na norma ISO 27002.
[37] ISO 27001, cláusula 6.1.3. alínea f), pág.4
[38] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 24, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

Só após a efetiva gestão de riscos ser completada é que será feita uma **auditoria**[39] para garantir que os riscos foram adequadamente tratados, da qual se retira a decisão de que foram implementadas as medidas apropriadas, sob pena de retoma imediata para o 1º passo de gestão até alcançar a elaboração de controlos mais satisfatórios. Caso a avaliação conclua que o risco é aceitável, isto é, que exista, mas que não afete a atividade organizacional nem coloque em causa os direitos e liberdades fundamentais das pessoas singulares, então o risco será considerado como gerido adequadamente. O resultado das auditorias nunca atingirá o patamar de risco zero, uma vez que o intuito da gestão de risco é torná-lo incapaz de colocar em causa os objetivos negociais, as pessoas, os processos e as tecnologias, ou seja, assegurar a convivência aceitável com a sua existência incontornável.

2.3. Relação Prática entre os Requisitos de Proteção e os Termos Analisados[40]

Qualquer ameaça pode afetar uma ou várias das componentes da segurança de informação, seja a confidencialidade, integridade e ou disponibilidade. A ocorrência de impacto proveniente duma ameaça só existe, como vimos, caso haja vulnerabilidades, o que é perfeitamente usual quanto maior for a densidade informativa contida no sistema. O nível qualificado ou quantificado de risco indica o nível de exposição da informação que possui um valor monetário ou lógico associado. À medida que a informação a proteger detenha um grau valorativo mais elevado fará com que o risco sofra, também ele, um aumento. Há, portanto, uma correlação inegável entre toda esta terminologia, a qual releva para a proteção de dados pessoais, essencialmente no que diz respeito à Privacidade desde a conceção, à segurança dos dados e a averiguação do dever de comunicar a autoridade de controlo ou de notificar o titular sobre a violação de dados pessoais e, essencialmente, para o desenvolvimento de uma Avaliação de Impacto sobre a Proteção de Dados Pessoais (AIPD).

Os requisitos e fundamentos de proteção têm o seu alcance por meio das medidas e controlos de segurança, mas são fruto do tipo de qualificação atribuída ao valor da informação

[39] Cfr. NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, págs. 5 a 8.
[40] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 3, ponto 12, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

e ao nível de risco. Se perspetivarmos uma informação de valor elevado para o negócio e um alto nível de risco (com exposição acrescida de ameaças e explorações de vulnerabilidades), então os requisitos de proteção carecem duma elevação extrema. Se tivermos perante a proteção de dados pessoais sensíveis[41], isto é, com valor elevado nos tramites do Regulamento Geral sobre a Proteção de Dados, mesmo que o nível de risco seja quase inexistente, estaremos perante uma conjuntura sem alarmismos, sem que os requisitos de proteção sejam levados ao extremo, mas devem estar alinhados a facto do valor da informação ser elevado. Deste modo, a projeção de que medidas de segurança devem ser concretizadas dependerá do cenário específico e de que organização esteja em causa.

3. Gestão da Segurança da Informação - Ocorrência do Incidente

O primeiro ativo estratégico para gerir a Segurança da Informação parte da elaboração da PSI que transmite as linhas orientadoras da direção, mas a mera elaboração desta norma geral não é autossustentável para o alcance dos objetivos de gestão da segurança da informação.

Na ISO 27001 é indicada, na cláusula 5.3, a necessidade de elaborar uma **estrutura e organização da Gestão** na qual sejam definidos nitidamente os papeis e responsabilidades[42] no Sistema, já que todo o conhecimento necessário para a Segurança da Informação não surge contido num único departamento especializado, tendo em conta o caráter multidisciplinar desta vertente que exige a envolvência de outras áreas (entre elas, a jurídica, financeira, de recursos humanos ou marketing). Caso haja um departamento específico de Segurança de Informação, com cargos especializados, com foco direcionado para a proteção da informação, maior será a maturidade da estrutura. A entidade pode até conter facultativamente um

[41] Designação equivalente às categorias especiais de dados pessoais (nos termos do artigo 9.º do RGPD), inicialmente suscitada pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (antecedente ao RGPD), nos considerandos 33 e 69, e, ainda referenciada pelo próprio RGPD no considerando 10.º in fine. Nas orientações WP 248 do GT29, os dados pessoais sensíveis (no critério 4.º para a verificação da obrigatoriedade da AIPD), são alargados para um elenco que não pertence aos categorizados como especiais no artigo 9.º do RGPD, abrangendo outros dados de natureza altamente pessoal, os quais se incluem as comunicações eletrónicas, dados financeiros, documentos pessoais, diários, *et cetera*. Portanto, no entendimento do RGPD e da legislação que o antecedeu, os "dados sensíveis" parecem se enquadrar nos elencados no artigo 9.º do RGPD, mas estes abrangem, inclusive, outras categorias que aumentam possíveis riscos para os direitos e liberdades dos indivíduos, designadamente os dados associados a atividades privadas e familiares ou que afetem o exercício de um direito fundamental e a vida quotidiana do titular dos dados.

[42] ISO 27001 cláusulas 5.1 alínea h) e 5.3 – págs. 2 e 3; ISO 27002 cláusula 6.1.1, pág.4.

Comité de Segurança da Informação e Compliance (CSIC)[43] com foco quer nos interesses negociais quer na tecnologia e respetiva segurança. Em patamares inferiores da hierarquia estão os utilizadores da Informação, enquanto manuseadores autorizados, onde são incluídos todos os funcionários e terceiros que utilizem a informação nas suas atividades laborais. A estes incumbe a responsabilidade de conhecer e cumprir a PSI na íntegra, sob pena de serem aplicadas sanções ou processos disciplinares previstos pelas Políticas Gerais instauradas pela organização. Importa reforçar que a acumulação de funções num único funcionário induzirá no risco elevado de uso indevido, pelo que as entidades devem seguir uma segregação funcional[44] para distribuir as responsabilidades conflituantes (por exemplo, ser simultaneamente gestor de acessos e utilizador).

Na estrutura documental, a PSI pode ser elaborada através de uma Política Geral, harmonizadora das regras gerais aplicadas a outras documentações derivadas, da qual derivam políticas específicas em documentos distintos. É uma estrutura facultativa, mas aconselhável ante um contexto vestido de múltiplas particularidades. A listagem de políticas derivadas pode ser vasta[45] dependendo do contexto organizacional, entre elas a Política de Gestão de risco, Política de Proteção de Dados, Política de Segurança Física, Política de Controle de Acesso, Política de Gestão de Incidentes, Política de Email e Comunicação Instantânea, Política de Desenvolvimento Seguro de Aplicativos ou até Política de Conformidade[46].

Tal como ocorre na fase de averiguação dos riscos, podemos preencher conhecimentos acerca da **Gestão de Incidentes de Segurança de Informação**[47] referenciada nas Normas ISO 27002, pelo que citamos o objetivo primordial**:**

> *"Objetivo: Garantir uma abordagem consistente e eficaz ao gerenciamento da segurança da informação"* ISO 27002, cláusula 16.1

[43] Grupo multidisciplinar composto por funcionários chave de cada departamento, que se reúne periodicamente para deliberar acerca desta temática e que serve como ligação entre a direção e o departamento específico de gestão de segurança. O objetivo é ter uma visão completa de todas as necessidades de Segurança da Informação relacionada com empresa. Exemplo prática da empresa NOS, primeira entidade certificada pela ISO 27001, consultado em https://www.nos.pt/institucional/PT/Sustentablidade/atuar/Paginas/Gestao-da-Seguranca.aspx

[44] ISO 27002, cláusula 6.1.2.

[45] ISO 27002, cláusula 5.1.1.

[46] Relativa a Direitos de Autor e Direitos Conexos, que assegura quais as fontes confiáveis para que o software seja adquirido, consciencializa sobre regras de uso de software e protege registos de propriedade intelectual (com auxílio de verificações periódicas, por exemplo), a que releva o Código do Direito de Autor e dos Direitos Conexos, Decreto-Lei n.º 63/85, de 14 de março.

[47] ISO 27002, cláusula 16, págs. 67 a 71 e com orientações específicas emanadas pela ISO 27035.

Segundo a terminologia, incidentes são "acontecimentos imprevisíveis[48]", isto é, ocorrências revestidas com conotação negativa que sucedem no sistema e que, com alguma probabilidade, venham a comprometer as operações e propriedades da Segurança. Nos termos da Lei n.º 46/2018 de 13 de agosto que transpôs a Diretiva (UE) 2016/1148, do Parlamento e do Conselho, de 6 de julho, o incidente define-se enquanto "evento com um efeito adverso real na segurança das redes e dos sistemas de informação (*cfr.* alínea c) do artigo 3.º da Lei n.º 46/2018).

Estruturalmente, os incidentes surgem na etapa antecedente ao dano propriamente dito, mas posterior à ameaça. A ameaça só se transforma em dano se o incidente vier a ocorrer, ou seja, se surgir a exploração prática da vulnerabilidade. Tomemos como exemplos a abertura dum documento PDF enviado via correio eletrónico e que danifica o dispositivo com a instalação de um vírus do tipo *ransomware*[49]; a transmissão de informações sigilosas num trabalho académico, pertencentes a empresa sem que esta tenha dado autorização para tal; ou uma base de dados acidentalmente apagada que afete a integridade ou disponibilidade da informação.

Na prática, a gestão de incidentes deve cumprir com determinadas etapas:

- Principia na identificação do incidente[50], seja por reporte do próprio utilizador ou por um analista especializado, seja por ferramentas de monitoramento;

- Segue-se o registo formal detalhado[51], por formulário ou através de ferramentas *Service Desk*[52];

---

[48] Definição disponível em: https://www.infopedia.pt/$acidente-ou-incidente?uri=lingua-portuguesa/incidente.

[49] Ataque de *ransomware* consiste no acesso ilícito aos sistemas computacionais e subsequente encriptação dos dados que só podem voltar a ser acessível à pessoa autorizada se for pago o resgate (normalmente, o pagamento é exigido por criptomoeda BTC). Mais camuflado será quando o pagamento seja exigido por criptomoedas dotadas de anonimização na transação, como os casos da *Zcash* e *Monero* que não permitem visualizar os endereços de envio e do beneficiário, além de não permitir a análise dos valores transacionados. Em Portugal, um ataque de *ransomware* tem enquadramento penal no facto típico de ilícito de extorsão (artigo 223º do CP) e no crime de acesso ilegítimo ou sabotagem informática nos tramites da Lei n.º 109/2009.
Cfr. MÁRIO ANTUNES e BALTAZAR RODRIGUES*, Introdução à cibersegurança* – a Internet, os aspetos legais e a análise digital forense, FCA, 2018, págs 127 e 128.

[50] ISO 27002 cláusula 16.1.2 – Orientação de Implementação – págs. 68 e 69.

[51] ISO 27002 cláusula 16.1.1 – Orientação de Implementação – alínea c), pág. 68.

[52] Unidade operacional que atua por registo de todas as entradas e saídas de suporte, com o objetivo de oferecer auxílio na gestão de incidentes e outras problemáticas de suporte à área de TI. Estabelece o único ponto de contacto entre parceiros negociais, fornecedores e clientes e é responsável por verificar falhas de segurança, gerir permissões de acesso, etc. Distinto do *Help Desk* (que soluciona problemas e fornece orientações de suporte destinadas ao utilizador final), a *Service Desk* resolve problemas de maior complexidade, entre eles a gestão de permissões de acesso, de problemas com servidores, verificação de falhas de segurança e outros aspetos que permitem um

- Prossegue na fase de classificação e priorização[53], através da rotulagem do incidente por tipologia, o que permite verificar se deve ser corrigido um incidente primeiro do que outros que decorram em simultâneo, com auxílio, para tal, de aspetos que determinem o seu nível de impacto-urgência. Da concretização do incidente podem advir impactos financeiros, operacionais, legais sancionatórios e/ou de reputação, que para serem devidamente calculados, implicam a adoção de fortes critérios de análise;

- Etapa de Diagnóstico inicial[54] com a primeira tentativa de solucioná-lo por análise de linha temporal (com verificação do seu começo e da forma como reagiram perante a implementação das medidas de dissuasão) ou pela técnica de Causa-Efeito[55]. Surge com a finalidade de retornar a Segurança no seu "nível normal";

- Conclui-se na Investigação Final[56] com diagnóstico que permita o seu tratamento por completo, de modo a evitar alastramento noutros dispositivos, através duma análise de causa-raiz (verificação do que permitiu que o incidente acontecesse) ou por ferramentas de análise automática.

Por questões inerentes à tipologia de incidente, ao seu nível de impacto-urgência e ao grau de experiência, posicionamento hierárquico ou capacidades operacionais de quem esteja a tratá-lo ou a identificá-lo, pode surgir no decurso da gestão do incidente um escalamento funcional ou um escalamento hierárquico[57]. O primeiro decorre quando seja necessário o encaminhamento do processo para outro responsável mais especializado na circunstância e o segundo quando o encaminhamento se justifique por exigir um nível de autoridade superior.

Após o seu tratamento importa criar um formulário-registo onde indique todos os aspetos essenciais relativos a este incidente com intuito de alcançar melhorias no Sistema de Gestão de Segurança da Informação e não pela mera atribuição de responsabilidades.

A gestão de incidentes na Segurança de Informação representa os processos de deteção, tratamento e avaliação dos incidentes[58] que impactem sistemas e comunicações. Na

registo mais completo e que olhe para as necessidades da organização como um todo. Disponível em: https://www.jitbit.com/news/helpdesk-service-desk-itsm/ e https://conteudo.movidesk.com/ferramentas-service-desk/

[53] ISO 27002 cláusula 16.1.4 – pág. 69.

[54] ISO 27002 cláusula 16.1.5 – págs. 69 e 70.

[55] Também denominada por "*Diagrama de Ishikawa*", permite representar a relação entre os efeitos decorrentes e as possíveis causas e, assim, localizar as causas mais prováveis, selecionando os detalhes relevantes para uma melhor análise – Técnica de investigar e neutralizar a causa real do incidente. Disponível em: https://www.mindtools.com/pages/article/newTMC_03.htm

[56] ISO 27002, cláusula 16.1.6, pág. 70.

[57] ISO 27002, cláusula 16.1.5 alínea c), pág. 70.

[58] ISO 27000.

área específica da Informação, a gestão requer considerações adicionais relativas à divulgação das informações acerca da ocorrência de incidentes (com intuito de evitar danos de reputação desnecessários para a empresa), ao controlo na propagação do incidente para outros dispositivos, além de dar seguimento a implicações legais específicas que condicionam a atuação face ao incidente, como por exemplo a obrigação de notificar os titulares de dados acerca da ocorrência de incidentes passíveis de comprometer direitos associados. Pese embora a importância de evitar a exposição das vulnerabilidades a agentes maliciosos externos que ainda não tenham conhecimento da sua existência, em algumas circunstâncias a legislação exige a notificação aos envolvidos[59] (à Comissão Nacional de Proteção de Dados enquanto autoridade de controlo, à equipa interna, fornecedores e clientes, isto é, os titulares de dados pessoais). Tal notificação deve ser projetada em prol da efetividade dos direitos dos titulares, mas importa não tornar público o reconhecimento dos incidentes por forma a não transmitir detalhes do sistema que possam comprometê-lo, nem quebrar a credibilidade da entidade em causa. Assim sendo, deve notificar sobre aquilo e a quem que for estritamente necessário, nos parâmetros legais.

Elucidando o impacto que pode advir de uma má gestão de incidentes, através dum caso real que decorreu em 2017[60], a empresa UBER assumiu publicamente ter pago o valor de 100 mil dólares para ataques externos apagarem dados de milhões de clientes e funcionários. Caso delicado já que envolve dados pessoais, entre eles os endereços de email e contactos telefónicos dos clientes contidos na Base de dados, possivelmente utilizados como alvos de ataques por *phishing*, além de envolver documentação pessoal dos condutores (seja cartas de condução, seja cartões de identificação). Além de consequências financeiras avultadas, este incidente fere a reputação da empresa e o âmbito operacional ao ponto do diretor de Segurança da UBER, Joe Sullivan, apresentar demissão. Neste caso concreto, a gestão de incidentes poderá não ter sido construída de forma correta, uma vez que se desencadeou a fuga de informação a esta escala (ressalvando que a Segurança absoluto é impraticável). Não existem dados concretos acerca dos danos diretos causados aos titulares dos dados pessoais, mas é nítida a ocorrência de danos indiretos, tais como a quebra de reputação da empresa

[59] Sob consideração dos artigos 33.º e 34.º do RGPD, das quais podem se socorrer contextualmente das linhas orientadoras do Comité Europeu para a Proteção de Dados (na terminologia inglesa, European Data Protection Board – EDPB) disponível em: Guidelines 01/2021 on Examples regarding Data Breach Notification | European Data Protection Board (europa.eu)

[60] Caso consultado em: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

quer para os clientes, quer para os funcionários. Com base no artigo referenciado, aparenta que não foi cumprida a obrigação de notificar as partes envolventes, mas que houve implementação de uma Medida de Correção (subsequente ao incidente e ao dano), já que a empresa disponibilizou gratuitamente meios de proteção acrescida para potenciais vítimas, particularmente, através de ferramentas de monitorização de transações.

4. Medidas de Segurança

Nos termos definidos pela ISO 27000, os controlos de segurança incluem processos, práticas e outras ações direcionadas a modificar o nível do risco que possa vir a impactar a Segurança da Informação, risco esse suscetível de análise numa fase anterior à aplicação concreta de medidas de controlo – **fase de análise e tratamento de riscos**. A aplicabilidade de tais medidas é justificada quando a realização duma atividade seja ou possa vir a ser afetada direta ou indiretamente pelo risco e que assim exija um controlo seguro. Surgem desde que não seja possível evitar a prática de tal atividade para que o risco seja dado como controlado. A modificação do nível de risco pode ter, como vimos, como fundamento a sua redução, a sua transferência (com o compartilhamento para outras organizações, por exemplo entidades seguradoras) ou aceitação, dependendo do que a Política Geral da organização considere como nível aceitável de risco. Para uma aplicação adequada dos controlos de segurança terá que conter não apenas as medidas técnicas, mas, em simultâneo, medidas no âmbito organizacional e de segurança física[61].

Partindo para uma análise pouco extensiva e detalhada, se perspetivarmos a vasta gama de controlos ilustrada na ISO 27002, elucidemos algumas das medidas dos três parâmetros para que se reconheça a sua imprescindibilidade.

[61] ISO 27002, cláusula 0.1 – Propósito e Contexto – "Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions.", pág. Vi, 5º parágrafo.

4.1. Medidas de Segurança Físicas

No âmbito das **medidas de segurança físicas**, o foco estará no controlo do acesso físico não autorizado e em potenciais interferências nas informações da organização passíveis de causar danos, através de barreiras de segurança apropriadas e projetadas para os riscos identificados, consoante a contextualização organizacional e respetiva exposição ao risco. Quando falamos de medidas físicas, o ponto primordial a ser protegido não é a informação, mas sim o funcionário enquanto ser humano que estará a trabalhar. Em consequência, além de ter em consideração a segurança da informação, as medidas são perspetivadas sob as orientações de regulamentos e normas de saúde, higiene e segurança no trabalho, tais como rotas de fuga bem sinalizadas, alarmes sonoros, além das instalações adequadas para proteção contra ameaças externas a que a organização esteja contextualizada, sejam incêndios, sismos, explosões ou perturbações da ordem pública[62].

Um exemplo prático de medida de segurança física é a elaboração de perímetros de segurança[63], a partir do anel externo à empresa protegido por barreiras da própria arquitetura do prédio com acessos supervisionados por vigilantes ou equipamentos de videovigilância e autorizados por meios de verificação eletrónica ou manual. Já na área de trabalho, mais aproximado ao ativo[64], poderá haver o controlo de acesso através da segregação de funções (com áreas de acessos exclusivos, consoante a tarefa a desempenhar pelo funcionário), acompanhada por equipamentos de monitorização, deteção de intrusões, etc. No *data center* as medidas devem ser mais rigorosas, com maior restrição de acesso, condicionado por biometria, por exemplo, ou com registo de data e hora de entrada dos colaboradores, como forma de aumentar o nível de rastreabilidade. A listagem de acesso autorizado a este perímetro mais sensível deve ser revista com regularidade. Quanto mais o acesso autorizado se aproxima do ativo, maior é o nível de sensibilidade, pelo que mais rigorosos devem ser os controlos de entrada física.

[62] Cfr. CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 25, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).
[63] ISO 27002, cláusula 11.1.1, pág. 31.
[64] Área designada para o processamento de dados e armazenamento em suporte físico ou eletrónico, como é o caso do *data center* onde são abrigados os sistemas computacionais e componentes associados.

Num panorama prático de segurança física em escritórios ou outras instalações similares, destaca-se que pela ISO 27002[65] é aconselhado ter em consideração os riscos de segurança de informação na fase preliminar, da própria construção ou aquisição do prédio. Os dispositivos sensíveis, onde ocorre armazenamento e processamento de dados, devem estar localizados nas áreas mais restritas, consoante o perímetro de segurança estipulado, não sendo lógica a sua exposição a áreas cujo acesso é menos condicionado (designadamente, a receção, as áreas de entregas, vendas ou carregamento de mercadoria), nem com proximidade a materiais perigosos e inflamáveis. Os edifícios em causa devem ser discretos, na medida do possível, quanto à sua finalidade e valor de informação que neles contenha. Melhor dizendo, é aconselhável evitar a exposição de letreiros desnecessários a agentes externos, já que a divulgação de informações facultativas (tal como a listagem dos funcionários com acesso autorizado a uma certa área ou dos departamentos existentes) facilita o atacante a mapear a empresa e a desenvolver ataques, por exemplo, um ataque de engenharia social[66]. Acresce ainda que a construção do edifício deve ser configurada de modo a ocultar informações confidenciais no interior, para que não sejam percetíveis visível ou audivelmente no espaço público.

Outra questão a elucidar no domínio de controlos físicos, associa-se à proteção contra ameaças externas relacionadas com o meio envolvente[67]. Se colocarmos em análise as consequências nefastas dum incêndio deflagrado podemos reconhecer a relevância de dispositivos móveis para a deteção atempada do incêndio, sem prejuízo das caraterísticas e considerações para a Segurança da Informação a ter em linha de conta, aquando da aplicação desses dispositivos[68].

Para que haja a combustão, é necessário existir oxigênio, calor e material inflamável – o denominado triângulo do fogo. No seu desenvolvimento, decorrem fases prévias à

[65] Cláusula 11.1.3.

[66] Nos ataques de Engenharia social, o atuador malicioso faz uma abordagem escrita ou oral, na qual se faz passar por outra identidade que não a sua – noção consultada através da hiperligação https://www.youtube.com/watch?v=SqI9cZx4974. Então, no caso de o atacante ter à sua disposição uma listagem de quem tem acesso a certa área sensível, poderá ser um mecanismo auxiliar para que este desenvolva um ataque oral de engenharia social, dependendo de que medidas físicas e organizacionais estejam implementadas para condicionar o acesso.

[67] ISO 27002, cláusula 11.1.4.

[68] Para se beneficiar de uma rede de objetos físicos, com componente eletrónica incorporada — baseada em tecnologias de sensorização e componentes de software embebidas — capaz de garantir a conectividade à rede e a troca de informação entre eles (Internet das Coisas, em inglês a denominada *Internet of things* (IoT)), o que implica conhecer os riscos e boas práticas específicas neste âmbito. Todavia a interligação plena entre sistemas informáticos e mundo físico será uma realidade, no futuro breve, que trará consigo aspetos positivos para completar a Segurança Física. *Cfr.* PAULO COELHO, *Internet das Coisas – Introdução Prática*, FCA, 2017, págs.2 a 7 e págs.211 a 230.

deflagração das chamas. Inicialmente, na fase de ardência sem chamas, se as instalações contiverem dispositivos de deteção tais como equipamento de aspiração do ambiente, será possível detetar a mudança das partículas no ar e enviar um alerta ou até combater automaticamente o incêndio. Na fase de fumaça, em que o perigo agrava, é determinante a existência do detetor ótico ou pelo detetor iónico. Nas fases de deflagração, com a situação crítica, há o detetor de chamas e o detetor de calor. Este tipo de controlo por dispositivos remotos permite detetar na 1ª fase de desenvolvimento de incêndio e poderá evitar a afetação direta ndo *data c*enter, além de desastres materiais ou humanos associados. Embora os custos sejam avultados para que uma instalação esteja totalmente equipada para combate a incêndios, quanto mais célere for a deteção através do dispositivo, maior é a probabilidade de evitar a ocorrência do dano. A sua distribuição tende a ser planeada consoante a criticidade, por exemplo, com a instalação do dispositivo de aspiração nos setores sensíveis (*data center* e, naturalmente, onde decorre o maior aglomerado de funcionários). Já espaços com menor criticidade, como espaços balneares, corredores e cantinas poderá ser suficiente a deteção de chamas e de calor.

E se os controlos de segurança física forem implementados de forma inadequada? Poderá desencadear falhas da infraestrutura física, casos de incêndio, explosão, inundações ou até acessos não autorizados. Uma empresa que não conte com um sistema adequado de segurança física terá, certamente, consequência nefastas na sua operacionalidade, nos seus objetivos negociais e, por conseguinte, na sua reputação. Por exemplo, se não for portadora de mecanismos de combate a incêndios, poderá sofrer uma sobrecarga elétrica que devaste todo o equipamento do *data center*. Neste caso, embora o impacto seja significativo, a retoma das operações da empresa dependerá da existência de controlos de segurança técnica adequados, nomeadamente a replicação na nuvem dos principais sistemas. Aqui estaremos a falar de uma possível perda da integridade dos dados (se não estiverem todos replicados por segurança), mas é certo que permitirá evitar a perda prolongada da disponibilidade dos dados[69].

[69] *Cfr.* CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 32, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

4.2. Medidas de Segurança Técnicas

No domínio das **medidas de segurança técnicas**, a objetividade da sua implementação centra-se no combate aos riscos que interfiram, por via eletrónica, nas propriedades da informação (confidencialidade, integridade ou disponibilidade) por intermédio da rede local, da *cloud*, de USB, etc. Para alcançar o nível de proteção apropriado ao contexto organizacional implica a combinação de múltiplos controlos técnicos específicos para cada **camada de segurança lógica da entidade**, a monitorização das mesmas para a detenção de anomalias (através de ferramentas próprias, nomeadamente a *Threat Hunting*[70] e *Threat Intelligence*[71] ou por intermédio da gestão de incidentes, painéis e relatórios) e a estruturação de respostas eficientes para serem imediatamente implementadas perante tal deteção. A extensibilidade do perímetro de proteção técnica varia nos termos da mobilidade, armazenamento e alcance da informação organizacional, o que pressupõe a verificação da forma como esta é acedida pelas partes autorizadas (por computador situado na organização, por computador pessoal, por intermédio de smartphones), como é compartilhada e por onde se encontra armazenada (pen drives, computação na nuvem, dispositivos remotos, etc). O nível adequado de proteção está, portanto, correlacionado com os riscos identificados e com a usabilidade da informação que a organização tem no seu histórico de operações. Tal como requer no domínio de controlos anterior, a sua implementação demanda que haja combinação das dimensões de pessoas, processos e tecnologias.

A abordagem de efetuar a proteção em camadas é similar aos perímetros definidos na segurança física. Reconhecendo que o perímetro de armazenamento e partilha da informação está cada vez mais extensível, é necessário elevar os controlos técnicos até onde se encontra a informação. Nas camadas de segurança lógica (domínio técnico) surge, com sensibilidade ascendente: 1- Perímetro ao qual a empresa contacta com o exterior (rede aberta), dependente de técnicas de Criptografia, *Firewall*, *Honey Pot*, técnicas de DLP (proteção contra fugas de informação/*Leaks*), etc; 2- Rede interna da informação com controlos técnicos específicos – *Firewall* interno, controlos de acesso remoto, técnicas de DLP, etc; 3- Estações

[70] Ferramenta de deteção de ameaças à segurança de informação.
[71] Ferramenta de reações automatizadas/ inteligentes por compilação de ameaças que tendem a surgir em múltiplas fontes além organizacionais.

de trabalho, onde o utilizador realiza a atividade laboral em que os controlos comuns são as atualizações de segurança, *Firewall* local, técnicas de criptografia e controlos de IPS/IDS local; 4- Aplicações utilizadas dependem de revisão do código fonte (quando esteja disponível), análise frequente de vulnerabilidades, *Firewall* de aplicação (WAF), técnicas de DLP, etc; 5- Dados e informações confidenciais, exigem controlos de gestão de acesso e identidade do utilizador, as cópias de segurança (*backup*) e as técnicas de criptografia[72].

O controlo técnico utilizado em todas as camadas lógicas que merece destaque entre os demais, pela sua importância, sobretudo, no âmbito de Segurança da Informação, é a criptografia[73]. Tendencialmente[74], garantir diversas propriedades, designadamente a confidencialidade, a integridade e a autenticação, enquanto identidade do remetente e do destinatário, a origem e destino da informação podem ser confirmadas pelo certificado digital[75] (no caso da criptografia assimétrica com chave privada na função de encriptação). Por outro lado, poderá garantir o não repúdio, por forma a que o remetente não possa vir a negar a intenção de criação e transmissão da informação, já que a este pertence a chave criptografada. A sua utilização no seio da organização, exige a elaboração de um documento que defina as regras de uso da criptografia (Política de Criptografia[76]), alistando a forma como são geridas as chaves de criptografia nos casos de perda ou acesso ilegítimo, como é feita a cópia de segurança dos dados encriptados e estipulando que medidas devem ser tomadas para evitar o seu uso indevido (em *malwares*, por exemplo). Relativamente aos deveres dos

[72] *Cfr.* CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 33, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

[73] Para proteger a informação, utiliza codificações derivadas de modelos matemáticos e cálculos baseados em regras (algoritmos) para transformar uma mensagem legível numa comunicação em formato criptografado, permitindo a sua leitura e processamento apenas aos possuidores da chave de criptografia (os legítimos destinatários). Enquanto o algoritmo possa ser público, a chave de origem e de destino é secreta para impedir que a cifragem seja revertida por intrusos. Se a chave for idêntica na função de cifragem e de decifragem, então a criptografia é simétrica. Inversamente, se se tratar de chaves distintas para cada operação, a criptografia é assimétrica com entrega de chave pública, mas que apenas possa ser descodificado o conteúdo pela chave privada e assim garante a confidencialidade. No caso de a chave privada ser a da encriptação, haverá a necessidade de garantir a autenticidade, a origem da informação já que o remetente é o único detentor da chave privada. Poderá ser unidirecional (função *hash*), quando o cálculo dos parâmetros do conteúdo da informação seja irreversível para o mesmo arquivo (valor aleatório que contem sempre os mesmos carateres), ou seja, focado na verificação da integridade da informação. Na prática, como a criptografia simétrica tem um desempenho eficaz será aconselhável a sua utilização em circunstâncias que não permitam a distribuição constante de chaves, como ocorre na circunstância de criptografar todo o *backup* ou toda a Base de dados. Já na Assimétrica, como é dotada de garantias em diversas propriedades, é muito útil em operações bancárias, transferências de arquivos em redes abertas, etc.

[74] Embora, quando a sua implementação não decorre corretamente, poderá desencadear vulnerabilidades exploráveis, comprometendo a Informação cifrada.

[75] Composto por elementos essenciais que permitem manifestar a autenticidade do documento, entre eles, a sua data de validade, dados do identificado, dados do órgão emissor da certificação (a sua assinatura digital) e chave pública do identificado. A sua utilização depende da infraestrutura de chave pública confiável (ICP), a qual permite estabelecer uma relação de confiança entre partes desconhecidas, através desse terceiro/intermediário confiável, transmitindo a sua credibilidade – aquele que emite e valida o certificado digital. A ICP é composta pela Autoridade Certificadora que assina e emite certificados digitais (pode até ser criada na própria organização) e a Autoridade de Registo que valida a identidade dos certificados. A proteção dos certificados digitais é fulcral, já que a sua utilização é equivalente a uma operação com assinatura da alta direção da entidade.

[76] ISO 27002, cláusula 10, págs. 28 a 30.

titulares de chaves, importaria uma análise reforçada do Regulamento n.º 910/2014, de 23 de julho, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, e o Decreto-Lei n.º 12/2021, de 19 de fevereiro, que assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014.

De uma vasta listagem de controlos técnicos, elucidemos, além da criptografia, as *infra* referidas na tabela abaixo.

Tabela 2 - Controlos Técnicos

- ***Firewall***[77]	Efetua a monitorização do tráfego de rede e é decisor quanto ao que deve ser permitido, consoante regras de segurança alistadas pela entidade, bloqueando o que esta estipule como não autorizado. Segmenta o ponto de contacto entre os ambientes de rede interna com rede externa. Verifica se a conexão está autorizada, por análise do IP de origem e IP de destino, por identificação de aplicações e utilizadores autorizados, quando estejam em causa protocolos orientados à conexão como é o caso do TCP/IP usado, por exemplo, pelo HTTP (na prática pode permitir o acesso exclusivo a uma aplicação, a quem tenha necessidade de seu uso para realizar alguma atividade laboral – pode inclusive limitar por carga horária).
- ***Host Firewall* (Local)**[78]	*Firewall* executado em qualquer dispositivo individual não dedicado, como é o caso de um equipamento laboral. É uma forma útil de proteção contra *malwares*

[77] ISO 27002, cláusula 12.6.1, alínea g) número 2), pág. 47 e cláusula 13.1.2, pág. 50.
[78] *Cfr.* CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 34, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

Tabela 2 – Controlos Técnicos (continuação)

	que tenham como ponto de partida hosts individuais, prevenindo a sua disseminação em toda a rede interna. NOTA: é medida complementar ao *Firewall* de rede (insubstituível), enquanto garante de uma monitorização mais específica. Auxilia o alcance do nível adequado de proteção quando um dispositivo da entidade esteja conectado fora da rede interna, seja na rede pessoal dum cliente ou do funcionário – acompanha a extensão do perímetro (inclusive na rede interna).
- **Sistemas de deteção[79] e Prevenção[80] de intrusões**	▪ IDS – Monitoriza o tráfego e é capaz de detetar uma anomalia e enviar um alerta ao administrador da rede, seja por tentativas de acesso indevido ou outros ataques (pode ser instalado na rede interna ou num dispositivo local)[81]. ▪ IPS – Monitoriza e deteta os ataques, envia o alerta ao administrador, mas é capaz de reagir automaticamente, com base na configuração adotada pela empresa, através do bloqueio do tráfego a partir da sua origem, redefinição da conexão ou por aniquilação de pacotes maliciosos (é executável na rede interna ou num dispositivo individual).
- **DMZ[82]**	Segrega o servidor que fica, por necessidade, na rede interna daquele que deverá estar exposto numa rede mais ampla e desconfiável, como o caso da internet. A

[79] ISO 27002, cláusula 12.4.3, pág. 45 e cláusula 13.1.2, pág. 50.
[80] ISO 27002, cláusula 12.2.1, pág. 41.
[81] *Cfr.* JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, pág. 185.
[82] *Cfr.* JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, pág. 95.

Tabela 2 – Controlos Técnicos (continuação)

	redução da exposição de serviços da rede interna na rede não confiável permite controlar o risco de explorações de vulnerabilidades.
- ***Honeypot***[83]	Recurso de rede (site ou servidor da organização) que tem a função de ser atacado ou invadido para identificar e coletar evidências de ataques usuais na empresa, por exemplo, a identificação da fonte de origem, servindo como base de aperfeiçoamento das regras do *Firewall* e dos Sistemas de Deteção e de Prevenção de Intrusões (IDS e IPS). O servidor exposto ("pote de mel" - sem atualizações de segurança ou por regras do Firewall incompletas) apresenta dados públicos e irrelevantes e não contém informações reais ou capazes de impactar a organização.
- **Proteção Contra Fugas de Informação *(comumente conhecido pela terminologia inglesa — Data Leak Prevention***[84]	Efetua a monitorização de dados sensíveis, isto é, os dados categorizados como especiais pelo artigo 9.º do RGPD, garantindo o acesso exclusivamente autorizado. A sua atuação tem por base a classificação e tipologia da informação previamente estipulada pela entidade. Só com essa classificação é que é possível o DLP entender quais as informações que são públicas (sem necessidade de bloqueios na transmissão, cópia ou armazenamento), quais as informações de uso interno (exclusivamente armazenadas no uso interno) e quais as confidenciais nas quais não deve permitir, por exemplo, a sua cópia para um *pen drive* ou armazenamento na nuvem. Pode, inclusive, registar e notificar o administrador acerca das

[83] *Cfr.* CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 37, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).
[84] ISO 27002, cláusula 14.1.1, alínea f), pág. 54.

Tabela 2 – Controlos Técnicos (continuação)

	tentativas de transmissão da informação confidencial, bloqueando a sua cópia para dispositivos externos.
- **Filtro Web**[85]	Controlo de acesso à internet, filtra o servidor, site ou aplicativo que pode ser acedido pelo utilizador (seja funcionário ou cliente). A equipa de Segurança de Informação terá o papel de bloquear o acesso a sites que contenham riscos elevados para a Segurança da Informação, mas todo o outro conteúdo será estipulado pela própria organização. Por exemplo, na hotelaria a configuração do filtro web pode permitir o acesso a sites de pornografia, deixando a critério do hóspede, mas sites que interfiram com dispositivos legais deverão, com caráter obrigatório, estar bloqueados (como o caso da pornografia infantil).
- **Controlo de Acesso à Rede** [86]	Garante que o acesso a recursos da rede seja apenas estabelecido por dispositivos compatíveis com as regras de segurança exigidas pela entidade, por verificação de atualizações de segurança do dispositivo, do seu mecanismo de antivírus incorporado ou outras ferramentas de segurança exigidas.
- **VPN (Rede Privada Virtual)**[87]	Cria uma conexão criptografada que passe de uma rede insegura e ampla até à rede interna da organização, protegendo contra os ataques de *sniffer* (observadores de tráfego e capturadores de pacotes que neste caso estarão criptografados) – a sua configuração pode limitar a categorização de conteúdo interno com acesso permitido desde a VPN, de acordo com a necessidade laboral de aceder remotamente[88]. Na prática, o

[85] Controlo para garantir a conformidade da orientação na cláusula 9.1.2, alínea a), pág. 20 da ISO 27002.
[86] Mecanismo de garante quanto à cláusula 9.1.2, alínea c), pág. 20 da ISO 27002.
[87] Mecanismo de segurança para a conformidade da cláusula 9.1.2, alínea d), pág. 20 da ISO 27002.
[88] *Cfr.* JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, pág. 93.

Tabela 2 – Controlos Técnicos (continuação)

	dispositivo conectado via VPN, tende a ser visto como parte integrante de uma rede interna (apesar do acesso proveniente do seu exterior).
- **Análise de Vulnerabilidades**[89]	Classificar e priorizar fragilidades dos sistemas da rede e fornecer à entidade aspetos de consciencialização e exposição do histórico de ameaças no ambiente laboral de forma a que os utilizadores reajam com prudência, sendo aspetos relevante para a realização de auditorias externas ou internas. A coleta de evidências dos riscos é feita através duma ferramenta apropriada e conclui-se com apresentação em relatório, onde são reportadas as vulnerabilidades que surgiram nos aplicativos, nos sistemas operativos, além das falhas de atualizações (e que uso foi dado a componentes desatualizados) ou erros de configuração, gerando o nível global de vulnerabilidade dos sistemas e ativos avaliados. É o controlo fundamental para identificar a exposição de fragilidades, mas não é ferramenta de correção.
- **Atualizações de segurança**[90]	Efetuar atualizações e correções de sistemas operacionais, aplicativos ou hardware com regularidade (em todo o ambiente organizacional) que, em alguns casos, acrescentam novas funcionalidades, é fulcral para a aplicação de correções regulares, imprescindíveis para manter a Segurança de Informação eficaz. Devem ser testadas antes da sua execução e, *a posteriori,* distribuídas, executadas periodicamente, com o impacto analisado. Todavia, a correção do problema de segurança poderá desencadear problemas relacionados,

[89] ISO 27002, cláusula 12.6, págs. 46 a 48.
[90] ISO 27002, cláusula 12.5.1, págs. 45 e 46.

Tabela 2 – Controlos Técnicos (continuação)

	por exemplo, perdas de capacidade de processamento – problemas de desempenho.
- **Cópias de Segurança (*backups*)**[91]	Processo de duplicação de dados que permite o seu restauro em caso de perda de integridade. Uma entidade pode conter o servidor de *backup* no espaço físico onde se encontram os dados alvo de duplicação (circunstância em que é aconselhável a sua replicação para outro espaço física), um servidor de *backup* remoto armazenado num lugar fisicamente segregado de onde estão os dados ou o *backup* na nuvem. Tipologicamente, a cópia de segurança pode ser: a) Completa, com cópia total dos dados, o que exige uma ocupação de espaço alargada em contrapartida do tempo de restauro eficaz como vantagem (com armazenamento seguro dos dados); b) Diferencial, que copia todos os dados desde a última cópia completa (estrategicamente utilizado após o *backup* completo e com periodicidade semanal). Exige um uso moderado de espaço e mantem o rápido restauro. c) Incremental quando copia apenas os arquivos de dados novos ou modificados desde a última operação de *backup*. O tempo de restauro será moderado, com menor eficácia posto que necessita de vários arquivos de *backup* para fazer a restauração completa, mas utiliza menos espaço que os tipos anteriores. O processo de cópias de segurança exige a sua formalização para que seja bem sucedido. Devem ser armazenados em locais seguros (complementados com

[91] ISO 27002, cláusula 12.3, págs. 42 a 43.

Tabela 2 – Controlos Técnicos (continuação)

	orientações e controlos físicos) e periodicamente analisados, surgindo implicações legais quanto ao tempo de retenção máxima de certas categorias de dados.

Nos controlos de ordem técnica, que riscos abarcariam no caso de falhas na sua implementação, monitorização ou execução? O Impacto nas operações, na segurança da informação e na privacidade da empresa pode ser muito elevado. Sucintamente, como consequências diretas das falhas de controlos técnicos podem surgir fugas de informação[92], acesso não autorizado, perda da confidencialidade, disponibilidade e integridade ou até espionagem industrial[93].

4.3. Medidas de Segurança Organizacionais

A execução consistente e uniforme das regras técnicas e de segurança física dependem de **medidas organizacionais** adequadas, ou melhor definindo, de orientações administrativas com a objetividade de suporte complementar para os controlos de segurança física e de ordem técnica, através da garantia de transmissão adequada (clara e inequívoca) das regras de Segurança de Informação entre as partes interessadas, por interposição das Políticas de Segurança de Informação, processos e regulamentações periodicamente revistos para permitir a sua pertinência contínua e contextualizada com a organização e riscos identificados. Têm, portanto, uma relação coadjuvante com os demais controlos.

Já foram elucidadas algumas das orientações administrativas fundamentais, como é o caso da Política de Segurança da Informação e a tarefa de consciencialização[94] e capacitação

[92] Caso da *Equifax* de fuga de informação (impacto muito elevado) expôs dados de, aproximadamente, 143.000.000 americanos. No comunicado da direção, refere que um funcionário do departamento de segurança de informação falhou em seguir os avisos de segurança e não garantiu a execução de uma correção disponível no software *(patch)*, permitindo a exploração da vulnerabilidade em causa - CVE-2017-5638 - ao ponto de afetar economicamente e em contexto de reputação da organização de um modo catastrófico. Em 2019, após conclusão do processo judicial de que foi alvo, a *Equifax* investiu numa plataforma para indemnizar as pessoas afetadas pela violação de dados, consoante os critérios de violação, com um *plafond* no valor de 575 milhões de dólares, 300 dos quais para fornecimento de serviço de monitorização de crédito para os consumidores afetados. O impacto económico pode ser, como vimos, abismal até sem entrarmos nos parâmetros legais sancionatórios.
Consultado em: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related ; https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement ; https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html ;

[93] *Cfr.* CLÁUDIO DODT *et alia*, 2018, *in ISO 27001: Curso completo para certificação EXIN ISFS!,* Secção 5, ponto 55, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável em julho de 2021).

[94] ISO 27001, cláusula 7.3. págs. 5 e 6.

dos colaboradores[95] da entidade. Na PSI são implementadas as orientações da alta direção, consoante requisitos negociais, legais ou regulamentares e graças a este ativo estratégico contextualmente elaborado, é protegido o compromisso contínuo do Sistema de Gestão da Segurança de Informação. A consciencialização[96] e capacitação[97] permitem alargar e aperfeiçoar o conhecimento das partes diretas na operacionalidade da entidade, quanto às regras adotadas para que sejam capazes de enfrentar ameaças e riscos identificados e associados ao cargo a desempenhar, consoante regras preestabelecidas. Na prática, a tarefa de consciencializar pode ser executada por intermédio de palestras, folhetos, *workshops* ou comunicados oficiais da alta direção. O seu alcance parte da enunciação formal das expetativas retiradas da PSI, de que controlos são executados e requisitos exigidos consoante os papeis e responsabilidades estipulados, além dos processos disciplinares internos que possam advir de atuações indevidas. É uma atuação que encaminha o êxito das medidas de segurança físicas e técnicas. Da mesma forma, é essencial para a eficácia prática da PSI, pois de nada serve deter estes controlos aperfeiçoados sem que se saibam praticá-los.

Outra orientação determinante para esboçar as medidas de segurança é a classificação formal da informação[98] efetuada pela própria organização. Os requisitos de implementação de controlos dependem da natureza da informação, da estruturação atribuída aos dados que visam proteger, consoante o seu valor, a sua sensibilidade, criticidade e requisitos legais. A tipificação usual da informação é entre a informação pública (sem consequências na mera divulgação), a informação de uso interno da entidade com acesso exclusivos e a informação confidencial, da qual se extrai impactos severos para a organização caso surjam incidentes (perda de confiança, reputação e imagem denegridas, perda de clientela e coimas avultadas). Todas as categorias são fulcrais e em todas serão protegidas propriedades da segurança da informação. Até na informação pública necessita de proteção quanto à sua integridade e disponibilidade, por forma a que tenha a sua utilidade (publicitária, de acesso a catálogos e às caraterísticas dos produtos ou serviços). Além de ditar que requisitos devem se preenchidos para a seleção e execução das medidas de proteção, a definição da informação permite

[95] Nos termos da ISO 27001, cláusula 7.2. alínea b) "ensure that these persons are competent on the basis of appropriate education, training, or experience;" e na Nota da mesma cláusula "Applicable actions may include, for exemple: the provision of training to, the mentoring of, or the reassignment of current employees; or the hiring or contracting of competent persons.", pág. 5.
[96] Perceção individual da consequência proveniente duma certa atuação; Habilidade de reconhecer o seu impacto.
[97] Treino prático efetuado à escala global na organização para capacitar os colaboradores a lidarem com ameaças e riscos.
[98] ISO 27002, cláusula 8.2.1, págs. 15 e 16.

distinguir quem será o responsável por realizar a tarefa da classificação e como será feito o apagamento adequado da informação (último ciclo de vida).

A gestão do acesso lógico[99] (consoante o Triplo A[100]) agrega-se ao parâmetro das orientações administrativas e é o mecanismo de garante para surgirem apenas acessos autorizados a recursos e períodos estipulados. O utilizador dotado de acesso lógico deve proteger as suas credenciais, não permitir a sua divulgação ou partilha, informar quando haja suspeita de comprometimento das credenciais de acesso e efetuar a utilização somente para as operações autorizadas circunscritas nas Políticas de Segurança de Informação ou estipuladas consoante a função desempenhada. A implementação de funções segregadas é também determinante nesta gestão para evitar modificações não autorizadas e o surgimento de erros não intencionais ou fraudes. Caso não seja possível segregar funções, implica a execução de controlos alternativos de monitorização.

4.3.1. **Privacidade e Proteção de Dados Pessoais**

Outra das recomendações enunciadas pela ISO 27002 que deve ser preenchida para que a organização possa estar em conformidade com a ISO 27001, passa pela elaboração de uma Política de Privacidade e Proteção de Dados própria da organização. De índole administrativa, esta medida, quando comunicada a todas as partes envolvidas no processamento da informação e acompanhada por uma estrutura de gestão de privacidade apropriada, permite o encaminhamento para a situação de conformidade da empresa para com os atos legislativos associados, o denominado estado de *compliance*.

O certo é que, para estar em conformidade, implica o preenchimento dos diversos requisitos legais e contratuais associados, entre eles, requisitos relativos à propriedade intelectual, à proteção de registos organizacionais específicos (nomeadamente, registos de base de dados, registos de logs de transações ou auditorias, etc) e imposições legais para com

[99] ISO 27002, cláusula 9.2, págs 21 a 24 e Cfr. JORGE GRANJAL, *Segurança Prática em sistemas e redes com Linux,* FCA, 1ª edição, 2017, pág. 172.

[100] Conceitos de Autenticação, Autorização e Auditoria. Autenticação enquanto procedimento fornecedor de identificação válido através dum código diferencial e distintivo, usualmente denominado por credenciais associados ao saber, à posse ou a algo que apenas a pessoa possa ser (seja palavra passe, certificado digital ou biometria). A autorização decorre contextualizada com a entidade, após a autenticação. O aconselhado é que o acesso concedido seja o estritamente necessário para desempenhar as atividades que incumbem ao colaborador (**Princípio do Privilégio Mínimo**). A auditoria específica do acesso lógico implica a compilação das operações efetuadas pelo utilizador após a autenticação e autorização, pois, ainda que o acesso seja permitido, existem atuações que não devem ser realizadas sem motivo justificativo, sendo a compilação de atuações muito útil para identificar casos de acesso desnecessário, indevido ou tentativas de fraude.

a criptografia a implementar[101], mas centremo-nos na conformidade com a Privacidade e Proteção de dados[102].

Portanto, a adequada gestão de privacidade implica que haja um intermediário a quem incumbe fornecer orientações à direção, aos colaboradores e aos utilizadores dos dispositivos acerca das suas responsabilidades individuais e que processos devem ser seguidos escrupulosamente. Nos trâmites legais, estamos a nos referir ao Encarregado de Proteção de Dados (ou *Data Protection Officer – DPO)* figura exigida nos termos dos artigos 37º a 39º do RGPD e pelos artigos 9º a 13º a legislação nacional[103].

A cláusula 18.1.4 da ISO 27002 reforça que "medidas técnicas e organizacionais apropriadas para proteger informações de identificação pessoal, devem ser implementadas"[104]. Medidas das quais tiramos partido das *supra* referenciadas para o efeito específico em análise. Com a imposição comunitária que obriga a adotação de medidas de segurança adequadas para a coleta, processamento e transmissão de dados pessoais, e que restringir, em alguns casos, a transferência dos dados pessoais para países terceiros, importa refletir que uma organização que esteja certificada (e portanto, conforme) as normas ISO 27001 é um ponto de partida fulcral para estar em concordância com algumas das imposições legislativas.

Existem outras normas ISO específicas da temática, designadamente, a ISO 29100[105] que fornece uma estrutura de privacidade com especificidades (princípios, responsabilidades e considerações) para o correto processamento da informação pessoal, a ISO 29101[106] que define a arquitetura para a estrutura de privacidade (concentrada nas preocupações dos sistemas tecnológicos e componentes a preencher para a sua implementação) e, mais recentemente, a ISO 27701[107] enquanto extensão das ISO 27001 e ISO 27002 para a gestão da privacidade, com requisitos e diretrizes específicas.

[101] Como decorre da Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, no que diz respeito à arquitetura de segurança das redes e sistemas de informação na administração pública.
[102] ISO 27002, cláusula 18.1.4, pág. 76.
[103] Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD.
[104] Na versão consultada, em inglês "*Appropriate technical and organizational measures to protect personally identifiable information should be implemented*" pág. 76, na cláusula 18.1.4 em "orientações de implementação", 2º parágrafo in fine – ISO 27002.
[105] Objeto consultado em: https://www.iso.org/standard/45123.html, aplicável a pessoas singulares e coletivas.
[106] Objeto consultado em: https://www.iso.org/standard/75293.html
[107] Consultado em: https://www.iso.org/standard/71670.html

5. ISO/IEC 27701:2019

Esta linha de orientação internacionalmente reconhecida parte da extensão do Sistema de Gestão de Segurança da Informação, emanado da ISO 27001 (requisitos) e 27002 (controlos de segurança), mas fornece diretrizes relativas à proteção da privacidade, de modo a facilitar a seleção e implementação de controlos por parte dos Responsáveis pelo Tratamento dos Dados Pessoais. A ISO 27701 suscita orientações para o alcance de um Sistema de Gestão da Privacidade da Informação[108] e não apenas de Segurança da Informação. Não basta proteger a segurança, mas sim a segurança estar complementada com a privacidade dos titulares dos dados pessoais. O auxílio ao estado de *compliance*, o direcionamento para alguns artigos do RGPD constitui o verdadeiro *leitmotiv* da Norma 27701. É uma norma autorregulatória capaz de encaminhar a empresa para o cumprimento de parte das suas obrigações legais neste contexto. Há uma garantia da Privacidade, enquanto objetivo final, através de técnicas de proteção de dados.

No ponto de vista conceitual, importa refletir sobre as dimensões que podem ser compreendidas na seção de "Privacidade". Por auxílio da designação decorrente do artigo 7.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE), relativo ao Direito de Privacidade, reconhece-se a ampla abrangência que o seu contexto pode alcançar, indo muito além da mera proteção de dados pessoais. O respeito pela Privacidade, implica o respeito pela vida privada, pela vida familiar, pelo espaço pessoal e pelas suas comunicações, pelo que faz incluir em setores distintos. Percorre a privacidade territorial, da qual faz limitar a intromissão no ambiente pessoal[109] do indivíduo; a privacidade corporal, associada à fisiologia, à genética, à biometria e aos atos corporais do indivíduo; a privacidade das comunicações, centrada nas correspondências pessoais por meios eletrónicos ou manuais; a privacidade da informação, que vai desde os registos de atividade no mundo cibernético[110] até aos dados pessoais financeiros, políticos, clínicos, entre outros.

Por remissão à definição de "Privacidade" plasmada na Política de Privacidade da IAPP[111], reconhece-se que "Em linhas gerais, a privacidade é o direito de ficar em paz, ou a liberdade

[108] Doravante, referido por SGPI.
[109] Na habitação particular, nos estabelecimentos laborais, ou até mesmo nos espaços públicos, já que estes também fazem parte da esfera jurídica do cidadão, mas não é por isso que possa estar sujeito a monitorizações automatizadas sem limitações e regras específicas.
[110] Através dos indentificadores por via eletrónica tais como os testemunhos de conexão – comumente designados por "cookies" – ou por endereços IP.
[111] International Association of Privacy Professionals.

de interferência ou intrusão. A privacidade das informações é o direito de ter algum controlo sobre como as suas informações pessoais são recolhidas e utilizadas."[112], entendendo o conceito como dinâmico no âmbito cultural e que definição poderá divergir, até mesmo nos direitos dos titulares.

Já no contexto do direito à proteção de dados pessoais enquanto direito fundamental específico[113], no n.º2 do artigo 8.º, constata-se que a proteção dos dados de índole pessoal implicará um tratamento leal, processado com fins específicos estipulados, que tenha por base um fundamento legítimo, como por exemplo o consentimento do próprio titular de dados pessoais, e que permita o acesso e a retificação dessas informações pessoais. Ora, o leitmotiv do RGPD, embora tenha sido alimentado pelo próprio percurso histórico, teve a influência imprescindível do artigo 8.º da CDFUE, ainda que não faça referência a este diploma. O certo é que, numa definição restrita de proteção de dados pessoais, podemos incluir diversos âmbitos de Privacidade expostos no artigo 7.º da CDFUE, nomeadamente a privacidade das comunicações e, sobretudo, a privacidade da informação, tipicamente reconhecida como Privacidade dos Dados.

Estruturalmente, o Ponto 1º da ISO 27701 indica o seu objeto. Não se direciona para a proteção de toda a informação, mas sim para a proteção de dados pessoais[114]. Na prática não estará em causa orientações para proteger, por exemplo, a base de dados associada ao stock, ou a lista de produtos mais vendidos representada de modo estatístico. São informações essenciais para a organização e, por esse motivo, devem estar rodeadas de Segurança de Informação, mas não são dados pessoais. Já se estiver em causa uma base de dados que exija mecanismos de gestão da privacidade (v.g. base de dados de clientes que utilizam a rede local, bases de dados dos funcionários, dos fornecedores ou dos clientes em geral), aí implicará o cumprimento da ISO 27701. A extensão do SGSI generalizado para o SGPI, está expressa no 5º ponto, no qual são adicionadas componentes de privacidade aos requisitos da 27001 e no 6º ponto que estende as diretrizes da 27002. No ponto 7 e 8, surgem diretrizes específicas para a atuação dos Responsáveis pelo tratamento e dos Subcontratantes[115].

[112] Disponível em https://iapp.org/about/what-is-privacy/ (consultável em julho de 2021).
[113] Cfr. SILVEIRA, Alessandra e CANOTILHO, Mariana (et alia) Comentário ao Artigo 8.º de CASTRO, Catarina Sarmento, in "Carta dos Direitos Fundamentais da União Europeia Comentada", Coimbra, Almedina, 2013, pág. 121.
[114] Conceito a descrever com maior detalhe no ponto 2.1. do Capítulo II.
[115] A terminologia correta será a denominação por "subcontratado", por acordo ao exposto nas orientações da CNPD, e não "subcontratante" enquanto terminologia adotada no Regulamento traduzido para a Língua portuguesa – *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, pág. 11, nota de rodapé 1.

Como tem sido ilustrado, a família de normas ISO 27000 é direcionada para a Segurança da Informação. Tal como a 27001, a ISO 27701 é uma norma certificável pela organização internacional de padronização em causa, o que significa que se a empresa implementar as suas orientações e pretender a certificação, passará por uma autoria oficial da ISO[116] e receberá a verificação que comprova como a empresa segue a melhor prática de proteção de dados, isto é, que atua nos tramites da norma internacional de privacidade. Não é requisito obrigatório deter a prévia certificação da ISO 27001 antes de se certificar pela 27701, mas há uma impossibilidade prática de garantir a privacidade sem ter segurança na informação em geral, já que para se certificar como dotada de um Sistema de Segurança com Privacidade, implicará o natural cumprimento das orientações da ISO 27001 e da ISO 27002. É este o motivo lógico que nos debruçamos até então na temática de Segurança de Informação em geral.

Legalmente, há uma obrigação imputada ao Responsável pelo tratamento de aplicar medidas de segurança aptas[117], de padronizações adequadas. Entende-se que a 27701 possa ser, atualmente, a metodologia que preenche parte deste intuito obrigacional, já que com esta se estabelece o padrão de privacidade em geral, ainda que não dite o cumprimento de obrigações específicas do RGPD (v.g. controlos obrigatórios em atividade do setor público, tipologia de criptografia a utilizar para um específico dado pessoal consoante a sua sensibilidade, etc.). Num sentido mais técnico operacional, as práticas para a gestão da informação em geral podem até ser complementadas através das orientações do DAMA-DMBoK 2[118], que direcionam para aspetos mais relacionados com a programação e o carater técnico dos controlos.

[116] O organismo certificador tem de estar credenciado de acordo com a ISO 17021-1, enquanto norma de avaliação dos organismos de certificação de sistema de gestão.
[117] Cfr. Considerando 78 e artigos 24.º, 25.º e 32.º do RGPD.
[118] DAMA *International Guide to Data Management Body of Knowledge* – disponível em: https://www.dama.org/cpages/body-of-knowledge (consultável em janeiro de 2021).

CAPÍTULO II – Conceituação do Regulamento e Relação Jurídica *Data* Protecionista

1. Contexto Histórico-Jurídico da Proteção de Dados

A proteção de dados pessoais é, inequivocamente, um tema que está na ordem do dia por fatores sociais, políticos e económicos que desencadearam a elaboração de legislação comunitária com abordagem modificada, direcionada para a segurança com privacidade rigorosa, comparativamente à abordagem antecedente. O intuito de proteger os dados não foi confecionado de raiz pelo Regulamento (UE) 2016/679.

No contexto europeu, o direito dos titulares à proteção dos seus dados pessoais tem a sua génese no artigo 8º da Convenção Europeia dos Direitos do Homem (CEDH) – direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência. Tal disposição legal exigia aos Estados Membros uma proatividade em prol do respeito da vida privada e familiar, o que implicaria uma atuação positiva na proteção de informações pessoais, temática à qual já se reconhecia valor económico intrínseco. Como consequência, surge, em 1981, a Convenção 108[119] que tomou como preocupações a forma como os dados pessoais eram recolhidos, tratados e as finalidades a que se destinavam no seu armazenamento e utilização, além de já determinar a distinção de dados pessoais sensíveis (relativos à raça, opinião política, convicção religiosa, orientação sexual, dados de saúde e registo criminal)[120].

Todavia, o primeiro instrumento jurídico comunitário direcionado exclusivamente para os Estados Membros, trata-se da Diretiva n.º 95/46/CE (de proteção de pessoas singulares no que diz respeito ao tratamento dos seus dados e a sua livre circulação) implementada pelo Parlamento Europeu e o Conselho, a 24 de outubro de 1995 e que seria transposta em Portugal através da Lei n.º 67/98, de 26 de outubro. A Diretiva de Proteção de dados veio harmonizar, de forma suficiente, as legislações estaduais, sobretudo no contexto do fluxo

[119] Atualmente, a Convenção 108 conta com "*51 Estados, incluindo os 28 Estados-Membros da UE, os quatro Estados da EFTA, todos os países dos Balcãs Ocidentais, vários países da vizinhança (como a Arménia e a Geórgia), a Federação da Rússia, a Turquia e vários países africanos (como o Senegal e a Tunísia) e da América Latina (Uruguai). Estão pendentes vários pedidos de adesão (por exemplo, da Argentina, do México e de Marrocos), tendo vários países o estatuto de observador (por exemplo, Japão e Coreia do Sul).*" – Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018PC0451&from=EN

[120] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 3 a 5.

transfronteiriço de dados por forma a que não surgissem entraves à livre circulação dos dados pessoais por razões de direitos e liberdades das pessoas[121]. Além disso, introduziu a criação de autoridades de controlo independentes como novos instrumentos de proteção, os quais viriam a estar incluídos na Convenção 108, após a sua alteração em 1999.

Como ponto de partida, o legislador europeu entendeu que seria suficiente implementar as normas comunitárias, sob a forma de Diretiva, numa temática à qual acrescem as reflexões e problemáticas consoante o mundo digital se desenvolve. Acontece que, com a entrada do novo século e o decurso das décadas iniciais, os Estados-Membros aperceberam-se que impor as obrigações legais da Diretiva seria uma tarefa um tanto impossível, posto que as próprias iniciativas legislativas estariam já ultrapassadas pelo decurso da era digital. As fronteiras digitais tornaram-se praticamente inexistentes, surgem as Redes Sociais, o Comércio Eletrónico atinge maior relevância, com volume de adesão impulsionado e as sociedades de informação sofrem transformações digitais por influência dos motores de busca digitais, dos dispositivos interconectados (Internet das Coisas), das *clouds*, do *Big Data,* entre outros. Foram transformações que levaram a que os dados pessoais passassem a ter um valor económico maior do que aquele que seria a realidade na década de 90. Conhecer a personificação do titular (os seus gostos, necessidades, tendências e hábitos de consumo) tornou-se uma vantagem fulcral para as organizações[122]. Para tal, o RGPD, há semelhança do que pretenderia a Convenção 108 e a Diretiva n.º 95/46/CE, considera que não deverá a livre circulação de dados pessoais ser restringida nem proibida por motivos relacionados com a proteção das pessoas singulares (*cfr.* n.º3 do artigo 1.º do RGPD). Deverá sim, garantir que a livre circulação de dados seja pautada por um tratamento lícito, leal e transparente, com respeito pelas disposições legais que do Regulamento se retiram, garantindo assim um equilíbrio entre os direitos dos titulares de dados e os interesses das pessoas coletivas.

Com a eminente necessidade de salvaguardar os direitos dos cidadãos[123], ficaria clara a necessidade de adaptar a legislação comunitária às novas realidades, por forma a aplicar homogeneamente, pelos vários Estados Membros, as políticas de livre circulação de dados

[121] *Cfr.* NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, págs. 11 e 12.
[122] *Cfr.* LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E para as organizações?*, FCA, 2018, *págs.* 23 e 24.
[123] Ressalve-se que após a proclamação da Carta dos Direitos Fundamentais da União Europeia (CDFUE), e após a sua vinculação como direito primário da UE com a aprovação do Tratado de Lisboa, em 2009, o direito à proteção dos dados pessoais ganha maior relevo de tal forma que passa a ser consagrado como direito fundamental no artigo 8º da CDFUE, havendo a sua distinção quanto ao respeito pela vida privada e familiar (estipulado no artigo 7º do mesmo documento legal).

pessoais na União Europeia. Para tal, não seria possível legislar, novamente, sob a forma de Diretiva que exigiria a transposição por cada Estado-Membro para ordenamento jurídico interno, com nuances, aplicações e procedimentos distintos. Para uma realidade sem fronteiras, implicaria a criação legislativa sob a forma de Regulamento, que se aplica diretamente, sem necessidade de transposição, a todos os países da UE e no Espaço Económico Europeu[124], impulsionando a Uniformização Legislativa nesta matéria[125]. Assim surge o Regulamento Geral sobre a Proteção de Dados (doravante, RGPD), aprovado no Parlamento Europeu e pelo Conselho Europeu (CE), no dia 27 de abril de 2016. Embora tenha por objetivo uniformizar os parâmetros de proteção de dados, detém aspetos aos quais os Estados podem transpor com limitações distintas, consoante a natureza jurídico cultural em causa[126].

O RGPD implicou uma mudança de abordagem, com fixação de novos direitos dos titulares de dados pessoais (como mecanismo de envolvência e capacitação dos cidadãos para impulsionar a vontade de exercerem tais direito, enquanto linha de preocupação motivadora para o Regulamento), aos quais passariam a ser exigidas novas obrigações para as entidades que tratam os dados pessoais, sob pena de abarcarem em coimas estrondosas[127] (o que estimula o cuidado acrescido e a inovação da Segurança da Informação nas organizações), além de novos elementos subjetivos obrigatórios na relação *data* protecionista, entre eles, o Encarregado de Proteção de Dados. Acrescente-se que os efeitos deste documento normativo abarcaram todos os dados pessoais que as organizações tinham em sua responsabilidade, inclusive os dados que tiveram o seu primeiro contacto de tratamento antes da entrada em vigor do RGPD. Perante tais circunstâncias, a efetiva aplicabilidade do Regulamento surgiu decorridos dois anos após a sua entrada em vigor (em concreto, a partir de 25 de maio de 2018), período esse que se considerou suficiente para a adaptação das organizações, de modo a alcançarem o estado pleno de conformidade para com as implicâncias do RGPD – estado de *compliance*.

[124] Além dos Estados Membros da União Europeia, o RGPD aplica-se diretamente à Islândia, Liechtenstein, Noruega e Suiça.
[125] Tal ponderação seria já transmitida com a elaboração do Regulamento n.º 45/2001 que não obteve os êxitos necessários para a respetiva harmonização.
[126] Vejamos o artigo 23º e os artigos 85º a 91º do RGPD. – *Cfr.* ANA FAZENDEIRO, *Regulamento Geral sobre a Proteção de dados*, Almedina, 3ª edição, 2018 *pág.* 10.
[127] Valor sancionatório com teto máximo de 20 milhões de euros ou 4% do valor de faturação anual das empresas. Foi através do agravamento das sanções, comparativamente à anterior legislação, que as entidades europeias entenderam como meio mais eficiente para trazer ao debate, e com máxima atenção, aqueles que tratam os dados pessoais.

A adequação dos dados pessoais à realidade cibernética atual pressuponha, ainda, o vínculo além comunitário às novas preocupações e nesse sentido, o regulamento intrometeu-se na relação dos dados pessoais com países terceiros (como veremos adiante). Por conseguinte, o Regulamento demanda um envolvimento global para que tenha efeitos práticos[128].

1.1. A Proteção de Dados Pessoais na Legislação Nacional

Nos **parâmetros legislativos nacionais**, precocemente existiu uma sujeição vincada a Portugal no que diz respeito às regras em matéria de proteção de dados, por ser Estado signatário de convenções internacionais, nomeadamente a Convenção 108. As origens jurídicas textuais de proteção de dados a nível nacional surgem na Constituição de 1976 no artigo 37º, sucintamente e muito centradas na informática, com referência ao direito de informação (isto é, o direito de informar, de se informar e de ser informado). Já na Constituição da República Portuguesa, desde a sua redação em 1976, surge a preocupação com a proteção do cidadão face aos riscos da informática. Vejamos, no seu artigo 35º cuja epígrafe se intitula em "Utilização da informática" veio estabelecer garantias ao respeito pela reserva da vida privada e familiar, quanto aos meios informáticos, preceituando a necessidade de proteger o cidadão face aos riscos postos pela informática, mas concretiza o direito à proteção de dados como sendo um direito fundamental[129] (note-se a influência do artigo 8º da CEDH, da Recomendação 509, de 1968 e, essencialmente das Resoluções 73/22 e 74/29, do Conselho da Europa). Portanto, são 45 anos de diferença entre a redação constitucional e o diploma comunitário do RGPD, mas que se encontram com similaridades surpreendentes: no n.º1 do artigo 35.º da CRP há já um desenho dos direitos do utilizador informático, aproximado ao do RGPD ao ser instituído o direito de acesso aos dados que lhe respeitem e esteja a ser tratados, a retificação e de atualização dos dados, além do Princípio da Limitação da Finalidade, aproximado ao Princípio da alínea b) do n.º1 do artigo 5.º do RGPD, enquanto direito a conhecer a finalidade dos tratamentos de dados; no n.º 2 do artigo 35.º da CP, surgiu uma listagem que, embora tenha sofrido alargamento nas revisões constitucionais, deteve a

[128] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs XIII a XVIII.
[129] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 9 a 11.

proibição do tratamento —enquanto regra — de um catálogos de dados, atendendo à sua sensibilidade, similares às atuais categorias especiais de dados do artigo 9.º do RGPD; sem demérito da previsão constitucional da instituição de uma autoridade administrativa independente introduzida no n.º2 do artigo 35.º com a 4.ª revisão constitucional, de 1997 e que coincide com a Autoridade de Controlo nacional — a Comissão Nacional de Proteção de Dados. Assim, desde a redação constitucional de 1976, o direito à proteção de dados pessoais segue construído com autonomia relativamente à proteção da reserva da intimidade da vida privada e familiar do artigo 26.º da CRP, permitindo a dignidade constitucional ao direito de proteção de dados pessoais, desde a sua versão inicial de 1976. Esse espírito pioneiro demonstra que "*o legislador constituinte (*teve) *por objetivo a garantia dos direitos e liberdades do cidadão na sua relação com a constante novidade das tecnologias de informação, comunicação e interação"*[130]

A jurisprudência do Tribunal Constitucional tem invocado, maioritariamente, os parâmetros do direito à reserva da intimidade da vida privada do artigo 26.º ou o direito de inviolabilidade/sigilo das telecomunicações do artigo 34.º[131], mas já recorreu diretamente à previsão do artigo 35.º da CRP para proteger o titular face a uso abusivo das suas informações pessoais, reforçando que o âmbito de proteção deste e daqueles direitos não ser coincidente — exemplificativamente, o Acórdão n.º 355/97 que se debruçou numa norma relativa à constituição de ficheiros automatizados com registos oncológicos, do qual o tribunal considerou que, embora fosse possível a invocação do artigo 26.º, já que estava em causa dados sobre a reserva da intimidade da vida privada (dados de saúde), recorreu ao artigo 35.º por estar em causa um tratamento automatizado dos dados.

Por forma a detalhar as preocupações que circundavam tal direito fundamental, foi elaborada a Lei n.º 10/91 reconhecida como a Lei de Proteção de Dados Pessoais face à Informática. O seu âmbito de aplicação estaria direcionado para os suportes informáticas que as Pessoas Coletivas utilizavam para armazenar os dados pessoais. Surge a criação da

[130] *Cfr.* artigo de CATARINA SARMENTO E CASTRO – *45 anos de "Utilização da Informática" – o artigo 35.º da Constituição da República Portuguesa, in* e-pública — Revista eletrónica de Direito Público, disponível em: https://www.e-publica.pt/volumes/v3n3a04.html.

[131] Nomeadamente, no Acórdão n.º255/2002 em que o tribunal constitucional apreciou uma norma que permitia a utilização de equipamentos eletrónicos de vigilância e controlo por parte das entidades que prestam serviços de Segurança Privada, com invocação do artigo 26.º da CRP; no Acórdão n.º403/2015 em que o tribunal constitucional apreciou a constitucionalidade de uma norma que admitia o acesso dos oficiais de informação do SIS, a dados de tráfego, de localização ou outros dados conexos das comunicações, com invocação do artigo 34.º da CRP; no Acórdão n.º241/2002 em que o tribunal constitucional apreciou uma norma que viabilizava ao juiz, em processo civil, a obtenção de dados de um trabalhador contidos em meios automatizados dos operadores de telecomunicações, designadamente os dados de tráfego, a faturação detalhada, et cetera, com a invocação, em simultâneo dos artigos 26.º e 34.º da CRP.

Comissão Nacional de Proteção de Dados Pessoais Informatizados (CNPDPI), a atual CNPD, que genericamente controlaria o processamento automatizado de dados pessoais, enquanto entidade administrativa independente tal como o nº3 do artigo 35º da Lei Fundamental o exigiu. Desde então, desencadeou-se uma série de bases legais[132] que descentraram o tratamento de dados pessoais exclusivo do âmbito informático e que desenvolveram a listagem de princípios fundamentais e um vasto leque de direitos à disposição dos titulares de dados, até atingir o ponto estabelecido pelo RGPD.

Há a execução para a ordem jurídica nacional por via da Lei.º 58/2019 de 8 de agosto, enquanto Lei Nacional de Execução do RGPD, que vem regular a sua aplicação[133] nas vertentes às quais o próprio regulamento estipulou serem fixados pelo direito dos Estados Membros.

Quer o Regulamento Geral, quer a Lei Nacional que o executa, não trouxeram consigo qualquer alteração de princípios em matéria *data* protecionista, mas garantiram a especificação de conceitos e a sua homogeneização prática, obrigando a reformular a abordagem à temática da privacidade e ao modo como desencadeavam o respetivo tratamento. Veio, portanto, assegurar o seguro controlo de um Direito Fundamental que se encontrava desfortalecido. Entenda-se "controlo" como exigência capaz de assegurar a projeção de uma Europa Digital[134], marcada pela livre circulação de dados pessoais dentro da União Europeia (e com restrições face à transferência para países terceiros), sem colocar entraves à modernização comunitária e à usufruição dos essenciais dispositivos digitais. Assim, o RGPD fica despido de restrições à utilização de dados, desde que essa utilização seja lícita.

[132] Por ordem cronológica, a Lei n.º28/94 que estabeleceu o direito de informação e acesso atribuído à CNPDI por forma a cumprir as suas funções; a Lei n.º67/98 que transpôs a Diretiva n.º95/46/CE para o ordenamento jurídico português, regulando a natureza, competências e funcionamento da CNPD (matéria que as normas comunitárias deixaram para as jurisdições nacionais adequarem consoante as autoridades locais); a Lei n.º 43/2004 que regularizou a organização e funcionamento da CNPD, sem revogar as competências e atribuições pré estabelecidas na Lei n.º 67/98.

[133] A listagem de especificidades reguladas pelo Lei Nacional de cada Estado Membro é vasta (entre elas, a nomeação da autoridade de controlo que no caso português é a Comissão Nacional de Proteção de Dados, a não carência de certificação profissional para se considerar um EPD, estabelecimento de regras para o tratamento dos dados pessoais de pessoas falecidas – artigo 17º da Lei Nacional, *ex vi* Considerando 27 do RGPD – prazos de conservação, condições para tratamentos específicos de dados pessoais, *et cetera*). Permite que haja um ajustamento administrativo-cultural, mas não abre brechas suficientemente capazes para quebrar a solidez da harmonização desejada.

[134] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 10, nota de rodapé nº5.

2. Tratamento de Dados Pessoais e a sua Licitude

2.1. Dados Pessoais

Partindo da perceção mencionada no 1.1 do Capítulo 1 *supra,* relativa ao conceito de Informação como a correlação de dados por si só, pessoais e não pessoais, está ciente que o *fulcrum* da legislação comunitária apela para o compromisso de Segurança da Informação com Privacidade, isto é, o controlo eficaz de todos os dados afetos a um respetivo titular, sendo a sua informação privada uma componente fundamental na esfera jurídica individual. O Regulamento 2016/679 veio aperfeiçoar a proteção de dados pessoais na prática, mas especificou com maior nitidez toda a conceituação relativa a esta matéria, se compararmos com a anterior Diretiva 95/46/CE. Descreve-nos os dados pessoais como sendo a "informação relativa a uma pessoa singular identificada ou identificável", isto é, " que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (…)"[135], pessoa singular essa que passa a considerar como a "titular dos dados".

Os dados pessoais são todos aqueles que identificam o titular sob a forma direta, quando identificam inequivocamente a pessoa que dizem respeito, sem serem necessárias informações adicionais, ou sob forma indireta que, embora não identifique autonomamente qualquer titular, permitem tal alusão, sem esforço considerável à luz de um juízo de razoabilidade, quando sejam correlacionados com outros dados. Ou seja, podemos conter dados da pessoa identificada explicitamente (v.g. o Nome completo, imagem, etc.), ou dados da pessoa identificável[136] (v.g. data de nascimento, profissão, etc.) que cumulativamente, pode vir a identificar a pessoa sem que sejam acompanhados de dados explícitos e diretos. Qualquer informação será considerada dado pessoal caso contenha detalhes sobre a vida privada ou profissional, sejam esses provenientes do passado, do presente ou do futuro. Exemplos claros de dados pessoais são os números que identificam o titular (civil, de

[135] Artigo 4º nº1 RGPD

[136] Por referência ao Considerando 26 do Regulamento, o Princípio da Razoabilidade para identificar se estamos perante uma "pessoa identificável" implica "considerar todos os fatores objetivos como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica", estando em consideração as circunstâncias casuísticas, os tipos de dados correlacionados e a finalidade para o tratamento dos dados em causa, para que na conclusão possa ser dada resposta à possibilidade ou não do Responsável (ou terceiros, nomeadamente outras entidades para quais os dados sejam emitidos) vir a identificar o titular por acesso a esses dados.

contribuinte e segurança social), o seu *curriculum vitae*, o seu estado civil, morada, entre outros[137].

No âmbito da Jurisprudência comunitário, têm surgido acórdãos que clarificam certos aspetos dos quais são considerados dados pessoais. Destaquemos os casos de: registo de espaços temporais laborais Ac. do TJUE C-342/12, (*Worten)*; imagens gravadas em vídeo no Ac. do TJUE C-212/13, (*Rynes)*; Observações de peritos divulgadas na internet acerca de determinados projetos Ac. do TJUE C-615/13, (*ClientEarth)*; Respostas em avaliações Ac. do TJUE C-434/16, (*Nowak)*. Esmiuçando o Acórdão *Nowak*, estaria em causa uma resposta de um exame de contabilidade, da qual, após concluída a sua efetuação, *Nowak* pediu as respostas efetuadas por si à instituição de avaliação, sendo que esta rejeitou por não considerar dado pessoal e, por isso, não teria o direito de acesso (artigo 15º do RGPD). Neste caso o Tribunal de Justiça da União Europeia clarificou que as respostas desenvolvidas em provas seriam consideradas como sendo dados pessoais, já que com base nas respostas é possível identificar a pessoa singular a que dizem respeito – titular identificável de dados pessoais.

Há um catálogo de dados ao qual a legislação denota maior apreensão e sensibilidade. São dados autonomizados como pertencentes à "categoria de dados especiais" e que se diversificam na licitude do tratamento[138], já que pode implicar um elevado risco de discriminação para o titular quando decorra o seu tratamento de forma ilícita. Em regra geral, fixada pelo artigo 9º do RGPD, é proibido o tratamento dos dados fixados neste leque sensível, sendo os relativos às opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, à origem racial ou étnica do titular, à vida sexual e orientação sexual, além dos dados genéticos, biométricos[139] e relativos à saúde que recebem a sua definição nos termos do artigo 4º nº 13 a 15 do Regulamento. Ao compararmos com o Convenção 108 do CdE, surge um alargamento dessa categoria fruto da evolução tecnológica e da exigência de uma eficiente proteção de dados, capaz de garantir os direitos fundamentais dos titulares e a não discriminação[140].

---

[137] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 30 a 39.

[138] Retratados no Considerando n.º 51 e seguintes e no artigo 9º RGPD, na sua maioria são os denominados em "categorias específicas de tratamentos" do artigo 8º da Diretiva 95/46/CE ou "dados sensíveis" já em legislação nacional desde a lei nº. 67/2008.

[139] Nos dados biométricos não estão incluídas as fotografias que não sejam processadas por meios técnicos que permitam a identificação inequívoca de uma pessoa singular – Considerando 51.

[140] *Cfr.* NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, pág. 59.

2.2. O Tratamento de Dados Pessoais

De modo a dar continuidade das bases concetuais a debater com maior foco, quando falamos de "Tratamento de dados pessoais", tal como o Regulamento estipula nos termos do número 2 do artigo 4º, estamos a referir-nos às operações, individuais ou conjuntas, efetuadas sobre um dado pessoal ou uma conjuntura de dados pessoais, quer de forma digital ou tecnológica, quer de forma manual. Para suscitar tal tratamento, a operação deve surgir exercida em função dos dados pessoais, em qualquer fase do seu ciclo vital[141], associados a uma pessoa singular, exemplificando as operações como "a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". Por isso, são pelo menos, segundo o Regulamento, dezoito operações diferentes que se podem considerar como tratamento. Fica escassa ou até mesmo nula a possibilidade de qualquer organização não estar submetida às exigências legais, quando atue perante dados pessoais sejam eles de fornecedores, de clientes e dos próprios funcionários e demais colaboradores.

A propósito, o artigo 4º nº2 ao estabelecer a interpretação de "tratamento" reforça a extensa margem de aplicabilidade material do dispositivo legal comunitário emanada no artigo 2º[142]. Entende-se por tratamento sujeito aos tramites do RGPD, qualquer operação que advenha de meios automatizados, total ou parcialmente, ou decorra de mecanismos não automatizados, no que diz respeito a dados espalhados em ficheiros no formato de papel. Esta aplicação material abrangente ressalva a necessidade de proteção global dos dados dentro da União Europeia*. A contrario* seria deixar uma brecha significativa para contornar as restrições impostas[143]. Além do mais, e como é de conhecimento global, afigura-se inevitável que nas atividades e relacionamentos com empresas ou outro tipo de organizações não se façam circular uma diversidade de ficheiros não automatizados. Perante o estabelecido, também a

[141] Desde a sua criação, armazenamento ou processamento, o transporte, a alteração ou eliminação.
[142] Todavia, o Regulamento suscita uma série de exceções à sua aplicabilidade material – no número 2 do artigo em análise – além de salientar no Considerando 18 que a sujeição do tratamento às suas exigências implica que este opere perante atividades profissional ou comercial, deixando de fora todo o "tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas", ais quais ilustra "a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades".
[143] Poderia até impulsionar o efeito inverso de desincentivo à modernização e usufruto das novas tecnologias nas organizações, já que na prática bastaria atuar sem meios automatizados para que estas não estivessem vinculada às exigências legais.

documentação em formato físico[144] fica vinculada à obrigatoriedade de implementar mecanismos adequados de proteção, que nestas circunstâncias se afigurariam aos tais controlos de segurança física a implementar nas instalações que garantam as propriedades de confidencialidade, integridade e disponibilidade dos ficheiros. Tal exigência implica uma gestão dos custos e proveitos que acarretam à organização, levando a questionar qual a formatação de dados mais conveniente no seio organizacional.

No procedimento de tratamento dos dados destaca-se uma mudança de paradigma consagrada com o RGPD, já que deixou de ser necessária a obrigação de notificar previamente a autoridade de controlo, no caso português a CNPD, para um controlo *a priori*, ou para uma autorização prévia que permitisse o tratamento de dados sensíveis (como acontecia na anterior Diretiva 95/46/CE e da Lei de Proteção de Dados 67/98, de 26 de outubro, *cfr.* artigos 18º a 20º e artigos 27º a 30º, respetivamente). Com o Regulamento atual, parte-se da presunção de que as entidades de tratamento são cumpridoras da legislação e é daqui que advém a obrigatoriedade de demonstrar uma contínua *compliance*, o que implica, neste parâmetro, que mantenham um registo atualizado desses tratamentos procedidos, por forma a demonstrar o cumprimento legal[145].

Ainda em relação ao tratamento, importa acrescentar a proporcionalidade patente no Considerando 4º do Regulamento 2016/679. O epicentro das preocupações relativas ao tratamento está na salvaguarda do direito à proteção de dados pessoais do titular, equilibrado proporcionalmente com os demais direitos e liberdades fundamentais do titular. Portanto, o direito à proteção de dados não é absoluto. Tomemos como exemplo as exceções à regra da proibição de tratamento de dados contidos na categoria especial, alistadas no nº2 do mesmo artigo 9º, para que se considere tratamento lícito de tais dados pessoais. Claro está o compromisso do Regulamento em controlar a utilização dos dados casuisticamente, o que não é sinónimo de total restrição da utilização de dados[146]. O que seria da vitalidade de uma vítima de acidente automóvel, que se encontre inconsciente e que dependa da rápida atuação de profissionais de saúde ou até mesmo dum cidadão comum? É factualidade óbvia que, mesmo sem o consentimento explícito do titular dos dados, os seus dados de saúde podem ser

[144] Considerando 15 do RGPD e *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, pág. 70.
[145] *Cfr.* ANA FAZENDEIRO, *Regulamento Geral sobre a Proteção de dados*, Almedina, 3ª edição, 2018 *pág.* 24.
[146] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, págs. 58 a 61.

tratados por proteção de seus interesses vitais. No âmbito nacional, é uma questão conflituante entre Direitos Fundamentais espelhados na Constituição, na qual um direito fundamental absoluto, como no caso *sub judice* o direito à vida, prevalece em detrimento do direito à privacidade e proteção de dados, respeitando o Princípio da Proporcionalidade e da Necessidade.

2.3. A Licitude, Lealdade e Transparência do Tratamento de Dados Pessoais

O caráter lícito, leal e transparente exigível ao tratamento é um dos Princípios que norteiam no número 1 do artigo 5º do RGPD. É esta a base de todo o sistema que o Regulamento vem consagrar e, sem demérito dos restantes Princípios associados ao tratamento de dados pessoais[147], parece-nos fulcral desenvolver o contexto deste princípio como pilar base aplicável ao tratamento, para que posteriormente se possa debruçar na adequação organizacional por via de implementação das exigências do RGPD[148].

2.3.1. **A Licitude do Tratamento[149]**

ALESSANDRA SILVEIRA realça[150] que "*Tratando-se de um direito fundamental sediado* (…) *no artigo 8.º é aplicável o regime que determina que: as restrições devem ser previstas por lei; devem obedecer ao princípio da proporcionalidade; devem corresponder a objetivos de interesse geral reconhecidos pela EU"* destacando que um tratamento de dados lícito cumpre as disposições que regulam direitos e fundamentos de legitimidade, mas também as exigências da Carta, nos termos do artigo 52.º da CDFUE.

[147] Nos termos do artigo 5º, refere-se ao Princípio da livre circulação, ao Princípio do propósito ou finalidade limitado(a), ao Princípio da minimização dos dados, ao Princípio da precisão e exatidão atualizada dos dados, o Princípio da Conservação ou limitação à retenção dos dados, o Princípio da Segurança dos dados e o Princípio da responsabilidade, sendo que estes vêm consubstanciar no vasto conjunto de direitos que acrescem aos já constantes dos artigos 12º e seguintes do Regulamento.

[148] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, págs. 30 a 34.

[149] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, pág. 44.

[150] *In* "Comentário ao artigo 52.º", pág. 592.

A concretização do caráter lícito do tratamento implica que no seu primeiro contacto com o dado pessoal – isto é, a recolha – detenha um fator de licitude que o fundamente. Por análise ao Considerando 40 do Regulamento, para que seja lícito, o tratamento deve surgir "com base no consentimento do titular dos dados em causa" ou, caso não surja por essa via, "noutro fundamento legítimo previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro". Assim, o tratamento poderá ser fundamentado por outros fundamentos legais que não o consentimento, designadamente, quando seja necessário para a execução de um contrato; para cumprimento de uma obrigação jurídica de que o Responsável pelo tratamento esteja sujeito; se necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; se necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública; para efeitos dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros; *et cetera*.

No comentário 4º ao artigo 6.º do RGPD[151], ALEXANDRE SOUSA PINHEIRO e CARLOS JORGE GONÇALVES, considerando, desde logo, que "*À exceção do fundamento associado ao consentimento* (…) *e, por isso, baseado na vontade do titular, os restantes fundamentos baseiam-se na lei, em contrato ou convocam a necessidade, enquanto dimensão do princípio da proporcionalidade*".

Assim sendo, o **consentimento**[152] do titular dos dados, cumulado com a determinação de uma finalidade específica, garante, que a recolha seja lícita, quando esta seja a base de licitude mais adequada. No número 11 do artigo 4º, o RGPD invoca um catálogo adjetival que o ato de consentir, enquanto manifestação de vontade, deve preencher para ser determinado como mecanismo de licitude, nomeadamente, o caráter livre[153], específico[154], explícito[155] e informado[156]. Essa mesma manifestação deve surgir através de um ato positivo inequívoco[157],

[151] *In* "Comentário ao Regulamento Geral de Proteção de Dados", Edições Almedina S.A., 2018, de ALEXANDRE SOUSA PINHEIRO (et alia), pág. 216.
[152] *Cfr.* LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E para as organizações?*, FCA, 2018, *pág.* 42.
[153] Quando o titular não esteja sujeito a qualquer pressão no momento da tomada de decisão. Há uma chamada de atenção, plasmada no artigo 7º nº4, quanto à circunstância de tal consentimento não poder ser considerado livre se, porventura, subordinar a execução de um contrato quando não seja fator essencial dessa mesma contratação. Para exemplificar, imaginemos um contrato de compra e venda em linha de um bem de mercado comum, no qual a sua execução dependa da transmissão consentida do grau académico completado pelo comprador. *A priori*, esse dado pessoal não se afigura relevante para a conclusão do contrato, pelo que tal "consentimento", ainda que transmitido pelo titular dos dados pessoais, não preencherá o caráter livre exigido pelo RGPD, sob pena de não garantir a licitude do seu tratamento.
[154] Completado com informação rigorosa.
[155] Quando a declaração de consentimento seja clara, sem cláusulas abusivas e fornecida de forma inteligível, demonstrando que o titular dos dados está plenamente consciente do consentimento que fornece.
[156] Titular informado sobre o objeto e as consequências do seu consentimento.
[157] O RGPD auxilia através do exemplo de manifestação dessa vontade através de uma declaração escrita, o que implicará o cumprimento de requisitos específicos alistados no número 3 do artigo 7º: "o pedido de consentimento deve ser apresentado de uma forma que o

do qual se retire a clara aceitação desse titular em tornar certos dados pessoais passíveis de tratamento. Poderá ter origem através de declaração escrita, oral, por validação de opção por via de um site *web*, ou por outra forma desde que indique a aceitação do tratamento proposto dos dados pessoais (pelo que o silêncio, omissão ou opções pré validadas não preenchem os requisitos de consentimento)[158].

O consentimento não será considerado base de licitude para o tratamento de dados pessoais quando o titular "não dispuser de uma escolha verdadeira ou livre, ou não puder recusar nem retirar a vontade de consentir sem que seja prejudicado" (Considerando 42 *in fine*), já que tal infringe a componente da livre vontade. Quanto à retirada da vontade de consentir, esta deve ser permitida ao titular em qualquer momento e surgir tão desburocratizada quanto a forma como possa ser fornecida, ainda que ao exercê-la não virá a comprometer a licitude do tratamento que teria sido previamente efetuado enquanto o consentimento vigorava. Tais factos encontram-se plasmados no número 3 das condições do consentimento (artigo 7º) e devem ser aspetos a informar ao titular antes de fornecer o seu consentimento. Para assegurar o caráter livre e verdadeiro do consentimento, "este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento "(considerando 43).

Pela sua ampla categorização no ponto 11) do artigo 4.º do RGPD e critérios de regulamentação plasmados no artigo 7.º do RGPD, o consentimento deverá seguir como última via de licitude para o tratamento de dados pessoais, paralelamente aos interesses legítimos que, como analisaremos *infra*, deverá ser utilizado com algumas cautelas.

Importa invocar outro contexto específico em que se interpreta a inexistência de livre vontade: o **contexto laboral.** Na relação laboral, o consentimento não releva como fundamento válido para tratar dados pessoais[159] consoante circunstâncias plasmadas no

distinga claramente de outros assuntos e de fácil acesso" (quando surja no contexto de uma declaração que manifeste, cumulativamente, a vontade sobre outros assuntos, nomeadamente, de vinculação contratual)", esteja elaborado "numa linguagem clara e simples" e não tenha cláusulas abusivas na sua redação (nos termos do Considerando 42).

[158] Considerando 32 do RGPD.

[159] Na relação laboral o tratamento de dados pessoais – excecionalmente permitido nos termos restritivos da lei, segundo os artigos 17º, 18º e 19º nº1 do Código do Trabalho *ex vi* artigo 28º nº1 da Lei n.º 58/2019 - terá por base de licitude uma finalidade específica (artigo 7º nº4 do RGPD) à luz das especificidades da relação (artigo 6º e artigo 9º, número 2 alínea b), ambos do RGPD). Por exemplo, consoante a apresentação ao empregador ou futuro empregador acerca do estado de aptidão ou inaptidão do trabalhador (alínea h do artigo 9º, número 2), é permitida por si só, mas não será se surgir a transmissão da ficha clínica (detalhada e justificada), ainda que seja dado o consentimento do trabalhador para tal. Importa saber se estará apto ou inapto para desempenhar as funções e não há razões para

número 3 do artigo 28º da Lei n.º 58/2019, posto que não é possível preencher a adjetivação que o legislador comunitário exige no consentimento. Há uma relação assimétrica entre o trabalhador e o empregador, isto é, o usual responsável pelo tratamento ou a quem se estabeleça forte ligação com este, pelo que apenas garante uma liberdade condicionada do trabalhador. Tendencialmente, poderá consentir por mero receio de represálias e por esta via o consentimento não poderá ser considerado.

Pela apreciação do "(…) *desequilíbrio próprio dos intervenientes típicos de uma relação laboral, e tendo em conta a referida necessidade de compatibilização dos interesses me conflito, o consentimento por parte do trabalhador não deverá, nem poderá, constituir fundamento de legitimidade para o tratamento dos dados pessoais deste.(…) não impede as entidades empregadoras de procederem ao tratamento de dados pessoais em contexto laboral quando outros fundamentos de legitimidade se manifestem*"[160].

A própria CNPD clarifica que o consentimento do trabalhador não será um fundamento de legitimidade idóneo, devido ao desequilíbrio da relação laboral que condiciona a caraterização do consentimento livre, além de que a larga maioria dos tratamentos de dados pessoais relativos aos trabalhadores estarem regulados por lei ou que sejam necessários para a execução do contrato de trabalho entre o empregador e o trabalhador[161].

Pelo exposto, numa apreciação aos restantes fundamentos jurídicos que legitimam o tratamento, nos tramites do artigo 6º da legislação comunitária, só será garantida a licitude se o tratamento surgir com caráter de necessidade. Portanto, será válido se o tratamento for estritamente necessário para **executar um contrato**[162], no qual o titular dos dados pessoais seja parte, ou nas diligências pré contratuais, a seu pedido. Haverá, ainda, condições de licitude quando o tratamento seja necessário para dar cumprimento a uma obrigação jurídicaque o responsável pelo tratamento esteja sujeito, como ocorre, por exemplo, do artigo 202° do Código do Trabalho, relativamente ao dever de manter o registo dos tempos de trabalho, em local acessível e por forma que permita a sua consulta imediata e que, neste contexto, o registo

detalhar o que motivou tal perspetiva – Artigo 19º nº3 do CT. Aqui pesa também o sigilo profissional a que incumbe ao profissional de saúde (artigo 9º, número 3 RGPD).

[160] No Artigo de SÉRGIO COIMBRA HENRIQUES e JOÃO VARES LUÍS, intitulado por "Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral", página 35, *in* Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2019, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf.

[161] *Cfr*. indicações disponíveis em: www.cnpd.pt/organizacoes/areas-tematicas/consentimento/

[162] Tomemos como exemplos o nome, número de contribuinte e residência para execução de um contrato de prestação de serviços públicos essenciais.

dos tempos de trabalho em que seja dada indicação, a cada trabalhador individual, das horas de início e de termo do tempo de trabalho, seria abrangido pelo conceito de dados pessoais – conforme decisão do TJUE no Acórdão C-342/12, *Worten*, ECLI:EU:C:2013:355, datado de 30 de maio de 2013 e, por isso, referente à vigência da Diretiva 95/46/CE. Dessa forma, o empregador estará obrigado a manter o registo dos tempos de trabalho de uma forma que possibilite a consulta imediata por parte das autoridades competentes, mas, em simultâneo, deve salvaguardar a proteção desse registo por forma a salvaguardar os dados pessoais (sendo esse o seu conteúdo). Poderá se fundamentar, por outro lado para serem cumpridas funções de interesse público ou por defesa de interesses vitais de qualquer pessoa singular[163].

Outro fundamento de licitude plasmado no artigo 6º, parte dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou terceiros desde que o responsável possa vir a "provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados" – Considerando 69 *in fine* - tendo em conta as razoáveis expetativas dos titulares dos dados na sua relação com o responsável[164]. Importa alguma cautela ao fundamentar o tratamento com base nesses interesses legítimos. O Regulamento tenta facilitar a interpretação através de exemplificações extensivas do Considerando 47, segundo o qual poderá ser considerado interesse legítimo o tratamento efetuado para efeitos de comercialização direta, quando esteja em causa uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento (como é o caso do titular de dados cliente ou do titular de dados colaborador do próprio Responsável), quando seja estritamente necessário aos objetivos de prevenção e controlo de fraude, entre outros.

Gera um certo grau de ambiguidade quando o fundamento, para que seja lícito, implique o reconhecimento das expetativas razoáveis do titular (sem entrarmos pela maturidade expetável de cada faixa etária) isto porque, o requisito de previsão razoável e expectável advinda do titular em saber que, "no momento e no contexto em que os dados pessoais são

[163] No caso de estarem em causa interesses vitais de outra pessoa singular que não o titular dos dados que estarão a ser, necessariamente, tratados, "só poderá ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico." – Considerando 46.

[164] Os interesses legítimos dos que são responsáveis pelo tratamento, só constituem fundamento jurídico para efetuar operações sobre os dados pessoais, desde que não prevaleçam os interesses, direitos e liberdades fundamentais da esfera jurídica do titular dos respetivos dados que carecem de proteção de dados pessoais. Um caso específico que não podem ser ponderados os interesses legítimos será quando a titularidade dos dados pertença a um menor de idade, posto que, por diversas componentes legislativas, trata-se do sujeito passivo com maior grau de proteção, nomeadamente a condição exclusiva de licitude – o consentimento emanado por titular de dados que já tenha completado 13 anos de idade ou, caso contrário, pelos representantes legais deste (consoante o artigo 16º da LGPD).

recolhidos", os seus dados poderão vir a ser tratados por motivos de interesse legítimo. Será o mesmo que reconhecer obrigatoriamente quando é que os titulares expectam ou não tratamento adicional por via desse fundamento - exigência modelada no Considerando 47. Assim, a justificação com base nos interesses legítimos deverá ser cuidadosamente planeada, o que requer uma avaliação casuística detalhada[165].

2.3.1.1. **Especificações da Licitude do Tratamento Categorias Especiais de Dados**[166]

Ainda que haja a proibição de tratamento dos dados sensíveis, plasmada no número 1 do artigo 9º, este poderá ser efetuado se for verificada alguma das exceções apresentadas no nº2. Essas derrogações à proibição de tratamento de dados especiais, vêm como manifestação reforçada de que o tratamento dos dados pessoais tem como papel primordial a salvaguarda dos Direitos Fundamentais em prol do titular dos dados (Considerando 4), no seu todo. Para tal, só através de nuances ao direito à proteção de dados pessoais é que será possível servir os titulares dos dados. Exige-se uma análise casuística desde às circunstâncias em que decorre e a função que o titular desempenha na sociedade, para que haja o equilíbrio de direitos fundamentais com respeito ao princípio da proporcionalidade[167].

As derrogações à regra geral garantirão a licitude do tratamento, na medida em que venham salvaguardar adequada e proporcionalmente um direito fundamental do titular ou de terceiros. Tal operação é autorizada em casos específicos definidos pelo Regulamento (artigo 9º número 2) e pelos Estados Membros de forma explícita.

De forma genérica, será permitido o tratamento de dados especiais quando haja consentimento explícito, pelo titular, para tratamento destinado a fins específicos, salvo se o direito comunitário previr que não pode ser anulada essa proibição; quando seja necessário para efeitos de legislação laboral, prestação social ou segurança social; no âmbito de atividades legítimas associadas a organizações sem fins lucrativos; se necessário à declaração,

[165] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, pág. 33.
[166] Tendo por base os dados pessoais especiais num âmbito do artigo 9º do RGPD, sem incluir os dados que provenha de condenações penais e infrações (artigo 10º), nem do tratamento automatizado de dados, por intermédio da denominada "definição de perfis" que segue exigências do artigo 22º.
[167] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, págs. 58 a 61.

exercício ou direito num processo judicial; para efeitos de medicina preventiva ou no trabalho; quando tal seja do interesse público[168] ou para fins estatísticos, de arquivo, investigação científica e histórica; por proteção de interesses vitais do titular, no contexto de estar impossibilitado de expressar o seu consentimento; quando seja necessário por motivos de saúde pública[169], destacando separadamente do fundamento de interesse público genérico, já que estará sujeito a condições específicas, nomeadamente a proibição desses dados relativos à saúde virem a ser tratados por terceiros – sejam seguradoras, entidades bancárias, ou, no exemplo já ilustrado, os empregadores - com vista a outras finalidades (dever de sigilo profissional e confidencialidade)[170].

Fica claro que, para cumprir a licitude do tratamento, implica equacionar as condições de licitude logo na sua fase embrionária e só assim é possível verificar o caráter de necessidade. E para que se proceda ao tratamento, o consentimento é um fundamento jurídico fiável no momento de apresentar a *compliance* da atuação *data* protecionista. No entanto, não se poderá sustentar e depender apenas dele para darmos andamento às diversas operações que o quotidiano venha exigir. Uma empresa não poderá pôr em causa a sua normal operacionalidade só porque não tem consentimento para tratar dados, já que urgem outras vias excecionais de validação jurídica para que estes sejam tratados, conforme o Regulamento permite[171]. De igual forma, no contexto pandémico que deflagrou no final da recente década, a monitorização da epidemia e o combate à sua propagação preenchem, em circunstâncias que assim a justifique, a recolha lícita de informações que se afiguram imprescindíveis por fins de emergência humanitária, servindo tanto por interesses públicos associados à saúde como, possivelmente, por interesses vitais do titular[172].

[168] Os considerandos 55 e 56 exemplificam as circunstâncias de interesse público quanto aos dados sensíveis, entre as quais serão no contexto da prática de atividades por autoridades públicas, de associações religiosas oficiais ou até no exercício das atividades eleitorais, desde que estabelecidas garantidas adequadas a proteção desses dados pessoais.

[169] A correta interpretação de "saúde pública" será segundo a definição do Regulamento (CE) n.º1338/2008 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho (JO L 354 de 31.12.2008, *pág.* 70) - *ex vi* Considerando 54 do Regulamento Geral de Proteção de Dados – designadamente "todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade".

[170] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, *pág*.36.

[171] *Cfr.* NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, *págs.* 37 e 38.

[172] Considerando 46, *in fine*.

2.3.2. **A Lealdade e Transparência do Tratamento**[173]

O preenchimento da lealdade pelo tratamento implica "*uma relação de equilíbrio entre responsáveis e subcontratantes e titulares dos dados pessoais. Pode manifestar-se de uma forma mais evidente em tratamentos de dados realizados por entidades públicas ou por empregadores*"[174].

Em parte, corresponderá a concordância efetiva por parte do titular que será exclusivamente atribuída através do consentimento válido, após ter sido informado acerca do objeto e consequências que envolverão tal operação nos seus dados pessoais. Prende-se, portanto, na concordância do tratamento por via do consentimento dotado de todas as caraterísticas que deve conter para se considerar válido (enunciadas no 2.3.1). Quando a lealdade seja posta em causa o ónus de demonstrar o consentimento caberá ao Responsável pelo tratamento, sendo relevante a preservação dos meios que tenha ao seu dispor para demonstrá-lo.

Com exclusão dos fundamentos de licitude excecionais supramencionados, é no consentimento válido que depende um objeto alvo de tratamento leal. Isso não quer dizer que o tratamento, por exemplo, por motivos de interesse legítimo, seja desleal em relação ao titular dos dados por não ter sido dada a concordância. A lealdade estará também ela preenchida se estivermos perante as circunstâncias excecionais do número 1, alíneas b) a f) do artigo 6º.

Para se considerar o tratamento como sendo transparente em relação ao titular dos dados, requer que as comunicações e informações relativas aos direitos que assistem o seu titular, questões inerentes ao tratamento[175] se mantenham com fácil acesso e compreensão, tendo em conta o contexto específico em que o tratamento seja efetuado. Tal requer que as informações sejam apresentadas no momento da recolha junto do titular dos dados, preferencialmente, pela via escolhida para fazer essa recolha do consentimento (e no caso de

[173] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 45 e 46.

[174] *Cfr.* Comentário 3.º ao artigo 5.º *in* "Comentário ao Regulamento Geral de Proteção de Dados", Edições Almedina S.A., 2018, de ALEXANDRE SOUSA PINHEIRO (et alia), pág. 207.

[175] Há obrigação de informar, com clarividência, acerca da identidade do Responsável pelo tratamento, as finalidades determinadas, específicas e legítimas a que se destina (ou quando haja intenção de tratar para fim diverso ao inicialmente destinado, salvo circunstâncias excecionais do Considerando 62), sobre aspetos que garantam a equidade do tratamento (nomeadamente os mecanismos de segurança implementados), sobre a ocorrência de definição de perfis e consequências que dela advenham, entre outras – Considerandos 39, 58 e 60 do RGPD.

serem obtidos a partir de outra fonte, dentro de um prazo razoável consoante circunstâncias, transmitidas pelas vias usuais de comunicação– correspondência postal ou via eletrónica)

Podem, inclusive, serem transmitidas as informações por combinação com ícones normalizados com o intuito de transmitir uma perspetiva geral do tratamento projetado. O certo é que há uma exigência incontornável de que a redação deve seguir uma linguagem simples, sem estar acompanhada de conceitos técnicos, complexos na sociedade comum, por forma a garantir o princípio da transparência. O próprio diploma comunitário diferencia a simplicidade linguística que devemos ter em conta no caso de informações e comunicações sobre o tratamento serem dirigidas a crianças[176].

A verificação do cumprimento dos princípios gerais do tratamento de dados pessoais, dando maior enfase no Princípio da licitude, lealdade e transparência enunciado no artigo 5º, nº1 alínea a), é o pilar base para auditar as operações de tratamento de dados pessoais efetuadas numa organização, tarefa que incumbe ao Encarregado de Proteção de Dados[177].

2.4. Os Mecanismos Adicionais de Segurança no Tratamento de Dados Pessoais – A Pseudonimização e a Anonimização

Nas operações de tratamento de dados pessoais, estes podem estar submetidos a um mecanismo de camuflagem de identidades por forma a que o seu titular não seja identificado.

É o caso da **Pseudonimização** elucidada no artigo 4º nº5 e nos Considerandos 28 e 29 do RGPD, em que os dados pessoais são, de tal forma, trabalhados em termos computacionais de modo a que não seja possível a atribuição ao seu titular específico (interpretemos pessoa singular identificada ou identificável) sem que para isso se recorra a informações complementares (cujas informações serão mantidas em separado e submetidas a controlos de segurança técnicos, físicos ou organizacionais para que não seja alcançada a identificação do titular, por cruzamento entre informação pública e informação privada). A ideia passa pela utilização dum critério técnico que irá substituir indicadores direitos e indiretos por valores com menor sentido associável à pessoa, embora estes possam novamente identificar o titular

[176] Considerando 58 *in fine*, RGPD.
[177] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, *pág*. 43.

quando haja acesso ao sentido lógico do critério de entendimento, às tais informações complementares[178].

Os dados pseudonimizados poderão ser utilizados para outros fins que não aqueles aos quais foram atribuídos o devido consentimento nos parâmetros da alínea e) do n.º4 do artigo 6.º. Além do mais, é um mecanismo auxiliar do tratamento quando o objetivo a ser procedido pela recolha da informação não exija a identificação do titular. Na prática, exemplificando, ocorre com regularidade nas informações com finalidades estatísticas ou de investigação científica, em que os dados existem e têm o seu efeito, cumprindo a sua finalidade, sem saber qual a pessoa singular identificável que transmitiu essa informação. A informação é guardada e protegida sem que, entretanto, seja apagada a informação associável e, inclusive, sem deixar que se torne anónima.

No caso da técnica de **anonimização**, por intermédio dos meios técnicos e organizacionais disponíveis, os dados não surgem acompanhados de detalhes que especifiquem a quem são associados, ou seja, não há *a priori* qualquer informação suplementar que tenha a obrigação de ser protegida separadamente por imposição do Regulamento. Um dado anónimo ou anonimizado é aquele que não é acompanhado por qualquer critério que capacite a identificação do seu titular[179]. Enquanto que nos dados anónimos nunca se interligou ao titular de dados que pertencem, os dados anonimizados, embora já não possam, em princípio, identificar o seu titular, estes foram submetidos a um processo de anonimização. Assim sendo, tanto a informação anónima como a anonimizada não se enquadrará no objeto material do RGPD, à luz do considerando 26.

Numa primeira abordagem, parece claro que um dado anónimo ou anonimizado seja o mais eficaz para garantir a proteção de dados pessoais, mas não é esse o entendimento correto a ponderar se analisarmos o artigo 25º nº1 e o artigo 32º, ambos do RGPD. O facto é que o dado pseudonimizado fica obrigado a vestir-se de toda a proteção jurídica emanada pelo Regulamento, o que não acontece no caso do dado anonimizado (excluído do âmbito do Regulamento pelo Considerando 26). Tal se justifica pelo facto de num dado anónimo ou anonimizado não haver possibilidade de identificar o titular, o que é sinónimo de impossibilidade de violação de dados pessoais, já que não se considera esta categoria de

[178] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, *pág.* 11.
[179] *Cfr.* LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E para as organizações?*, FCA, 2018, *pág.* 38.

informação enquanto dado pessoal. É usual ocorrer a anonimização na recolha de opinião acompanhada apenas por meros detalhes estatísticos (género, faixa etária ou outros).

Há a exclusão do Regulamento, tendo por base uma noção teórica, mas cientificamente é questionável a sua total eficiência. Parece-nos que, embora os dados anonimizados não se associem a uma pessoa singular, isso não deveria ser impeditivo de estarem sujeitos à carga regulatória da legislação *data* protecionista. Enquanto haja a anonimização na sua plenitude, os dados não têm a atribuição suficiente para identificar com precisão aquele a quem pertencem, mas não é por isso que os dados pessoais deixam de existir.

Aliás, a técnica de anonimização é contextual e momentânea. Nada garante que tal técnica seja, em todos os casos, inquebrável no futuro e que não possa reverter a identificabilidade do titular. Ilustremos através do caso de preenchimento de formulários/ questionários de forma totalmente anónima. O certo é que, a maioria dos formulários seguem um processo de anonimização, não sendo informações anónimas com tendem a indicar, mas sim anonimizadas. É exemplo quando estes são preenchidos, por via eletrónica, através dos dispositivos pessoais ou dos utilizados em espaços laborais, em que o próprio endereço IP (protocolo internet) poderá comprometer a identificação do titular de dados, ou até mesmo aquando da inserção de credenciais caso sejam necessárias para dar entrada numa plataforma de acesso aos formulários, por exemplo. Até se perspetivarmos o preenchimento manuscrito do formulário, não esqueçamos que a própria caligrafia ou a forma como selecionamos opções poderão ser suficientes para a identificação do titular (nuances biométricas, comportamentais).

Se recuarmos às Diretrizes sobre Técnicas de Anonimização (Opinião 5/2014) emanadas pelo Grupo de Trabalho do artigo 29º da Diretiva 95/46/CE[180] nas quais se estipulou que as bases do processo de anonimização devem revestir uma absoluta impossibilidade de reidentificação, "tão permanente quanto a eliminação"[181], reforçamos a intuição do legislador comunitário beber destas considerações ao estipular, no princípio da limitação da conservação dos dados pessoais, que após o período necessário para fazer valer as finalidades para as quais surge o tratamento dos dados, o Responsável pelo tratamento deverá proceder

[180] O Grupo de trabalho do Artigo 29º para a Proteção de Dados (GT 29), ou designado por "*WP*" devido à sua denominação em inglês *Article 29 Data Protection Working Party (WP),* veio a ser substituído pelo atual Comité Europeia de Proteção de Dados Pessoais, segundo o Considerando 139 do RGPD.
[181] Opinião 5/2014 do GT29, pág 6.

ao apagamento ou, alternativamente, promover a sua anonimização[182], o que faz equivaler a expetativa do processo de anonimização à natural eficácia da eliminação dos dados.

No entanto, esse caráter de irreversibilidade efetiva que a noção europeia abraçou no que diz respeito ao processo de anonimização, aparece, no RGPD, com índole maleável ao se encontrar delimitada pelo conceito de identificabilidade. Torna-se, portanto, problemática a sua exclusão de forma tão fragilizada, sobretudo no âmbito das técnicas computacionais de anonimização de dados que não são capazes de evitar totalmente a descoberta dos seus titulares – reconhecia-se já a anonimização como revertível, ainda que por meras probabilidades (risco omnipresente).

Segundo AUGUSTO CESAR TORBAY, "(…) *consagrar um conceito de anonimização que se carateriza, necessariamente, por uma dimensão omnipresente de risco poderá revelar-se particularmente problemática, principalmente se mantivermos presente que os dados anonimizados contornam a tutela consagrada pelo RGPD."* Além de que "(…) *a consagração de uma noção frágil de anonimização poderá concorrer para o desenvolvimento de um ambiente de insegurança jurídica, como resultado da possível frustração das expetativas depositadas na viabilidade das garantias prestadas pelo processo de anonimização*."[183]. Assim, a abertura a uma ponderação de razoabilidade de meios, faz-se afastar, de forma problemática, da noção absoluta de anonimização, tornando o processo complexo, quando acompanhado com os contributos científicos que denunciam a sua fragilidade incontornável, já que a reidentificação do titular estará pendente de um juízo de razoabilidade eminentemente subjetivo, não sendo uma impossibilidade objetiva – dimensão omnipresente do risco residual. AUGUSTO CESAR TORBAY acrescenta que "*(…) por se compaginar na realidade volátil e mutável do ecossistema digital e tecnológico, o critério de razoabilidade de meios poderá encontrar-se vazio de conteúdo, uma vez que poderá ser impossível determinar o que é, num dado momento, efetivamente razoável e, em última análise, poderá contribuir*

[182] Contendo a mesma equiparação no regime consagrado na Diretiva 2002/58/CE, no n.º1 do artigo 6.º.
[183] No Artigo de AUGUSTO CESAR TORBAY, intitulado por "A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia", página 57, *in* Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2020, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf.

para o desenvolvimento de um ambiente de incerteza por parte dos responsáveis pelo tratamento e de desconfiança por parte dos titulares dos dados"[184].

A interpretação mais lógica, tendo por base a *ratio* da norma, é que o legislador comunitário excluí a anonimização como sendo uma técnica aconselhável para proteger os dados pessoais, mas quando essa venha a existir, nada impede do Responsável pelo tratamento, nos parâmetros da sua Gestão do Risco, se precaver da possibilidade de vir a infringir sobre a proteção de dados pessoais, já que a viabilidade da anonimização dependerá de um equilíbrio entre a utilidade e o risco residual. Ademais, pelo nível de risco constante, o processo de anonimização deverá, inclusive, ser acompanhado de um comprovativo de que o titular dos dados pessoais tem consciência do nível de risco e que o aceita enquanto operação de tratamento dos seus dados, por forma a se reconhecer a fragilidade da anonimização e se promover a correta implementação de uma política transparência e com base no consentimento[185].

Assim, são mecanismos de segurança adicionais e que fomentam inúmeras vantagens para a Segurança da Informação, desde a diminuição do risco de danos causados por eventuais fugas de informação - os dados alcançados seriam não identificáveis, pelo menos por si só - além da possibilidade de evitar ou reduzir a aplicação de coimas por falta de proteção de dados desde a conceção (*cfr.* artigo 25.º do RGPD*)*. Mas, claro está no Considerando 28 *in fine* que "A introdução explícita da "pseudonimização" no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados", reforçando o caráter adicional de segurança e não de autossuficiência deste mecanismo.

São técnicas que, tal como se conclui do ponto 2.2 Gestão dos riscos (Capítulo 1), não devem ser encaradas como inquebráveis. Haverá sempre o incontornável Risco de Proteção de Dados Pessoais, nem que seja a longo prazo. Portanto, quer as técnicas de pseudonimização, quer mesmo as técnicas de anonimização não são aplicações suficientes para impedir a sujeição às exigências legais, desde o processo de adequação até à pós-atuação dos auditores de dados, como analisaremos adiante.

---

[184] No Artigo de AUGUSTO CESAR TORBAY, intitulado por "A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia", página 75, *in* Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2020, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf.

[185] *Cfr.* ponderações do artigo de KHALED EL EMAM, intitulado por "Does anonymization or de-identification require consent under the GDPR?", *in* IAPP, 2019, disponível em: https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/.

3. Relação Jurídica *Data* Protecionista

Por forma a direcionar o entendimento acerca da figura do Encarregado de Proteção de Dados, torna-se incontornável expor, ainda teoricamente, a relação jurídica que releva em matéria *data* protecionista.

3.1. Elemento Subjetivo Ativo – O Titular dos Dados Pessoais

O tratamento de dados pessoais, enquanto objeto do Regulamento, tem a sua composição numa relação jurídica protagonizada por uma pessoa à qual é fornecida direitos em prol da sua privacidade – o titular dos dados pessoais, enquanto elemento subjetivo ativo, isto é, dotado de direitos que forçam às obrigações, em contrapartida, dos elementos subjetivos passivos. No seu sentido lato, o titular é todo aquele que, por referência a um identificador, possa vir a ser identificado (artigo 4º alínea 1)) direta ou indiretamente. Ora, o legislador comunitário consagra a noção restritiva de titular de dados pessoais para efeitos do Regulamento, abrangendo apenas as Pessoas Singulares por via do Considerando 14. A restrição ao domínio de pessoas físicas, é um dos traços que reforça o *leitmotiv* da aprovação desta legislação comunitária, enquanto normativo centralizado nos cidadãos e seus direitos.

O preenchimento da figura de titular de dados pessoais, elemento central do Regulamento, não se esgota pelo mero facto de ser uma pessoa singular detentora de dados pessoais diretamente identificados ou indiretamente identificáveis[186], mas antes, implica a concretização de nuances para que este venha a ser protegido nos tramites do RGPD.

Primus, a sua aplicação implica que o titular seja, territorialmente residente[187] num Estado-Membro da União Europeia. Há uma extensão aplicável, não apenas aos cidadãos comunitários, mas a todos os que residam na UE. Aliás, se é tão verdade que o cidadão comunitário é, regra geral, detentor dos direitos do Regulamento (nos termos do artigo 3º

[186] Cf. *Supra* 2.1. Dados Pessoais.

[187] A expressão "residente no território da União Europeia" veste o critério de direito fiscal, isto é, a pessoa que tenha permanecido num Estado-Membro com intenção de ser residente habitual e de cumprir com as obrigações tributárias, sem também esquecermos dos seus dependentes (menores ou sem rendimentos suficientes para que cumpram com deveres subjacentes ao IRS). *Cfr.* LUÍS ANTUNES, *Pôr em Prática o RGPD – O que muda para nós? E para as organizações?*, FCA, 2018, *pág*. 29.

nº2), verdade será que o cidadão não comunitário será, também ele, detentor dos mesmos direitos, mas na dependência de estar perante um Responsável pelo tratamento ou subcontratado estabelecido no território da União ou em território cuja circunstância tenha aplicação de direito de um Estado-Membro por força do direito internacional público (artigo 3º nº1 e nº3).

Secundis, tal pessoa singular poderá ver o exercício dos seus direitos dependentes de atuações de terceiros, naturalmente. Se estiver em causa uma criança enquanto titular dos dados pessoais, o Regulamento exige uma proteção especial, encarando esses titulares como "menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais" (Considerando 8) e, para que o tratamento se torne lícito no âmbito de oferta de serviços da sociedade de informação às crianças, implica que a criança tenha completado 16 anos de idade (limite comunitário). Caso contrário, ficará à mercê do consentimento facultado validamente pelos titulares das responsabilidades parentais da criança – artigo 8º nº1. No ordenamento jurídico português, a LNE reduz, através do artigo 16º, a idade mínima de tratamento lícito para 13 anos (o equivalente ao limite mínimo exigido pelo Regulamento e colocado à disposição dos normativos de cada Estado-Membro – artigo 8º nº1 *in fine*).

Por outro lado, se os dados pessoais sujeitos a tratamento pertencerem a uma pessoa falecida, que façam parte da categoria especial de dados (artigo 9º do RGPD) ou quando façam parte da intimidade da vida privada, da imagem ou a dados relativos às comunicações, os direitos de acesso, retificação e apagamento, poderão vir a serem exercitados por pessoa designada para o efeito ou, na ausência de designação, pelos respetivos herdeiros (artigo 17º nº1 e 2 da LNE). Embora o Regulamento exclua as pessoas falecidas do seu âmbito de proteção[188], a Lei Nacional alarga a sua proteção até ao intervalo *post mortem*, deixando nas mãos do titular a possibilidade de determinar o não exercício desses direitos (artigo 17º nº4 LNE) ou de designar uma pessoa para o efeito. Caso não se prenuncie ficará a cargo dos herdeiros.

Tertius, a prepotência dos titulares para usufruir dos seus direitos não se esgota na sua natureza singular, localização e capacidade jurídica, mas antes no seu comportamento

[188] Considerandos 27, 158 e 160 do RGPD.

proativo para garantir o direito à proteção contra intromissões de terceiros na vida privada. Há, portanto, uma atuação pertinente que recai indiretamente sobre o elemento protegido, que implica o reconhecimento dos seus direitos, da relevância incutida nesta temática perante a atualidade digital (acompanhada de riscos, consequências e garantias) e o enquadramento nos contextos em que a proteção da sua privacidade releva no quotidiano pessoal[189]. Só através do comportamento ativo de *stakeholders* (e não apenas dos elementos cujo Princípio da Responsabilidade e os deveres de fiscalização e cooperação recaiam, como analisaremos de seguida) é que é possível dar azo à relevância do RGPD na prática[190].

3.1.1. **Direitos dos Titulares dos Dados**

Aos titulares dos dados pessoais que preencham a proteção atribuída pelo Regulamento, adquirem um conjunto vasto de direitos não consagrados ou sem a devida explanação em legislações anteriores (os *data subjects*, em inglês). De forma elucidativa, os titulares de dados pessoais são detentores dos Direitos à proteção dos dados pessoais (artigo 1.º), à informação (artigo 13.º), de acesso (artigo 15.º), de retificação (artigo 16.º), ao apagamento dos dados e a ser esquecido[191] (artigo 17.º), além dos direitos à limitação do tratamento (artigo 18.º), à notificação (artigo 19.º), de portabilidade dos dados (artigo 20.º), de oposição (artigo 21.º), à não sujeição a decisões automatizadas (artigo 22.º), a ser avisado sobre a ocorrência de violação de dados pessoais (artigo 34.º) e os direitos relacionados com os Princípios do tratamento de dados pessoais (artigo 5.º), enquanto pedra basilar do novo RGPD[192].

Estabelece-se novos direitos e disposições aos que outrora existiam, por forma a aumentar o nível de proteção do titular de dados. Todavia, como já frisamos com auxílio do Considerando 4 do RGPD, não estamos perante um catálogo de direitos absolutos e será

[189] Já que o conceito de "titular" alarga-se aos objetos que possuímos. São nos equipamentos tecnológico – *smartphone,* GPS, carros inteligentes e outros objetos desenvolvidos pela nova tecnologia da IoT – que ocorrem a maior partilha de dados pessoais.
[190] Embora surja um natural acréscimo de pedidos de informação e participações registadas pela CNPD (no seu Relatório de Atividades 2019/2020 apresenta um registo de 4577 pedido de informação e 2732 participações), o facto é que só através do mediatismo da temática é que suscitará o interesse do titular sobre os seus próprios dados pessoais para se alcançar a proatividade imprescindível.
[191] É um dos novos direitos que surgiram através do Regulamento e que nos termos jurisprudenciais do acórdão "*Google Spain*" do Tribunal de Justiça da União Europeia (Processo C-131/12 de 13 de maio de 2014), indica a permissão ao titular dos dados de solicitar ao Responsável pelo tratamento o apagamento dos seus dados. Tal determina a obrigação do Responsável pelo tratamento em informar aos restantes responsáveis que tenham os dados na sua posse (quando dados já tenham sido tornados públicos) da intenção de apagamento de todas as ligações para esses dados, emanada pelo titular "*assim como das cópias e reproduções, tomando as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação*".
[192] *Cfr.* ANA FAZENDEIRO, *Regulamento Geral sobre a Proteção de dados*, Almedina, 3ª edição, 2018 *págs.* 44 a 51.

necessária uma conciliação de direitos fundamentais, quando conflituantes, por intermédio de um critério de proporcionalidade.

Peguemos no contexto da Administração Pública[193]: os cidadãos têm o direito constitucionalmente consagrado à informação administrativa, seja informação procedimental (que diga diretamente respeito ao particular) ou não procedimental (que não lhe diga respeito) – artigo 268.º nº1 e nº2 CRP. É um direito inteiramente ligado ao Princípio da Administração Aberta, centrada no acesso livre e geral dos documentos administrativos (artigo 17.º CPA e artigo 2.º da Lei de Acesso aos Documentos administrativos[194]). Assim, regra geral, qualquer cidadão tem direito de acesso à informação não procedimental, sem que para isso tenha que apresentar justificação. Mas este direito tende a conflituar com o Princípio da Proteção dos dados pessoais – artigos 17.º e 35.º CRP e artigo 18.º CPA. Os documentos nominativos (aos quais estão contidos dados pessoais que careçam de proteção – artigo 3.º nº1 alínea b)) fazem gerar restrições ao direito de acesso e assim, um conflito de Direitos constitucionalmente consagrados.

Para solucionar este conflito, deverá suscitar-se uma articulação entre a LADA, o RGPD e a LNE (mais concretamente, o seu artigo 26.º). Importa distinguir-se os documentos nominativos que deem acesso a "dados gerais" (no contexto do artigo 6º nº9 do LADA[195]), dos normativos que contenham dados especiais (por remissão ao artigo 9.º nº2 do RGPD, poderá haver circunstâncias excecionais à proibição de acesso). Se tivermos perante uma conjugação necessária entre o Direito de acesso e a Proteção de Dados Pessoais Gerais (isto é, não pertencentes à categoria de dados especiais), será aplicável a presunção do acesso emanada no artigo 6.º nº9 da LADA. Para o funcionamento da presunção, teremos que aplicar o artigo 6.º nº5 da LADA e, dessa forma, o acesso a documentos não procedimentais nominativos só é possível com a existência de uma autorização escrita, explícita e específica por parte dos titulares dos dados (alínea a) do artigo 6.º nº 5 da LADA), ou, na sua ausência, o terceiro requerente terá de comprovar que é titular de um interesse legítimo, pessoal e direto suficientemente relevante[196] ao ponto de justificar o acesso à informação (alínea b) do artigo

[193] *Cfr.* JOSÉ RODRIGUES e DANIELA TEVES, *A Proteção de Dados Pessoais e a Administração Pública – o novo paradigma jurídico*, AAFLD, 2020, *págs.* 123 a 148.
[194] Lei n.º 26/2016, de 22 de agosto, doravante, designada por LADA.
[195] Inserido pelo artigo 65º do Capítulo IX da Lei nº 58/2019.
[196] Ponderação articulada com o Princípio da Proporcionalidade – artigo 18 nº2 CRP – e com articulação dos Direitos Fundamentais que estão em causa e de que forma se conjugam com o Princípio da Administração Aberta.

6.º nº5 da LADA). O auxílio do artigo 6º nº5 deve-se ao facto de ser pouco verosímil que a presunção faça inverter o ónus da prova para a Administração Pública.

Caso haja o conflito entre o Direito de acesso e a Proteção de Dados Pessoais Sensíveis ou Equiparados[197], teremos que ter em conta que, regra geral, o acesso é proibido, já que se sujeita ao disposto no Regulamento. Assim, para aceder a esses dados importará a existência de consentimento explícito, que esse dado seja manifestamente público por opção do titular, ou por outras conjunturas alternativas retiradas do Artigo 9.º nº2 do RGPD, na medida da restante legislação existente na UE ou no Estado Membro.

Em ambos os casos, a resolução não se poderá cingir na estrita letra da lei, exigindo uma avaliação casuística e por respeito ao Princípio da Proporcionalidade enquanto medida de resolução de conflitos (artigo 18 nº2 CRP). Conforme o Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, Processo n.º 7613/09.3TBCSC.L1.S1 "*são frequentes as colisões entre direitos fundamentais* (…) *há de ser solucionados pelo poder judicial mediante a respectiva ponderação e harmonização, em concreto, à luz do princípio da proporcionalidade, evitando o sacrifício total de uns em relação aos outros e realizando, se necessário, uma redução proporcional do âmbito de alcance de cada qual*"[198].

O certo é que nenhum direito fundamental deve ser suprimido ou totalmente negado por estar em conflito com outro. Devem consistir em função dos interesses em causa. Em última instância poderá ser solicitado um parecer à Comissão de Acesso aos Documentos Administrativos (CADA)[199]. Quando esses documentos nominativos estejam sujeitos a restrições de acesso, deverá ser feita uma comunicação parcial, através de uma expurgação da informação relativa à matéria reservada (artigo 6.º nº8 da LADA), isto é, retirada da informação que não se releve necessária para a finalidade invocada, analisando a possível afetação ao direito à privacidade. Caberá aos organismos públicos[200] proceder à análise inicial da necessidade de vedar ou permitir o acesso aos documentos administrativos nominativos,

[197] Dados contidos na categoria especial de dados da redação do RGPD e os dados relativos à intimidade da vida privada (previstos na LADA, apesar de não estarem contidos na categoria especial de dados, são equiparados).
[198] *Cfr.* Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, Processo n.º 7613/09.3TBCSC.L1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/-/A4AD03AAA6D9342780258O7A00589B2F;
[199] Com a coexistência da CADA e da CNPC, há um dever de harmonização entre as orientações que estas comissões distintas publicam, por forma a não deixar soluções distintas e que se recorra à mais conveniente, quer por parte do titular, quer por parte do Responsável pelo Tratamento ou Subcontratados.
[200] No caso das entidades públicas, são beneficiariam da faculdade de solicitar a dispensa de aplicação de coimas, devidamente fundamentada, durante três anos nos termos do artigo 59.º da LNE, quando contra estas decorra tal sanção findo o processo de natureza contraordenacional, sob o poder de apreciação discricionário conferido à CNPD – sob o disposto do artigo 44.º, n.º2 da Lei n.º 58/2019 e sob clarificação interpretativa na deliberação/2019/495 da CNPD.

devendo cingir a informação a ser fornecida ao estritamente necessário consoante a finalidade invocada.

Assim sendo, os direitos dos titulares, essencialmente o Direito à proteção de dados pessoais, podem ser sujeitos a restrições por conflituarem com outros direitos fundamentais, seguindo as exigências do artigo 18.º da CRP. No entanto, cada direito do titular é acompanhado por limitações específicas próprias redigidas nos artigos correspondentes, mas ainda sujeito a possíveis medidas legislativas nacionais ou comunitárias que restrinjam quaisquer desses direitos, por força de motivações referidas no artigo 23.º do RGPD[201]. Tais limitações comuns não poderão desrespeitar a essência dos direitos e liberdade fundamentais (artigos 17.º e 18.º da CRP), devem ser fundamentadas com base na salvaguarda necessária de valores pertencentes a uma sociedade democrática (alíneas do artigo 23.º nº1 do RGPD[202]) e, quando necessário, conter disposições explícitas relativas sobre os aspetos alistados, taxativamente, no número 2 do artigo 23.º do RGPD. Tais limitações deverão respeitar as exigências da Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais (*Cfr.* considerando 73 do RGPD).

3.2. Elemento Subjetivo Passivo – Responsável pelo Tratamento e Subcontratado[203]

A noção jurídica de titular dos dados pessoais possuí uma componente relacional incontornável, posto que a subsistência dos direitos dos titulares implica a existência de uma contraparte nos tratamentos da relação *data* protecionista.

[201] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, pág. 64.

[202] Em consideração com a alínea g) "A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;", o TJUE, no Caso IPI, Acórdão de 7 de novembro de 2013, proferido no Processo n.º C-473/12, declarou que "a atividade de detetive privado que atua por conta de um organismo profissional para investigar violações às regras deontológicas de uma profissão regulamentada, no caso, a de agente imobiliário, é abrangida pela exceção prevista no artigo 13.º, n.º1, alínea d), da Diretiva 95/46", alínea essa que se aplicava nos mesmo moldes que a alínea g) do n.º1 do artigo 23.º do RGPD.

[203] A terminologia correta será a denominação por "subcontratado", por acordo ao exposto nas orientações da CNPD, e não "subcontratante" enquanto terminologia adotada no Regulamento traduzido para a Língua portuguesa – *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, pág. 11, nota de rodapé 1. Tal tradução para a língua portuguesa poderá suscitar desvios interpretativos. Todavia, neste caso não será fator para desencadear desvios de conteúdo da norma, o que já acontece quando comparamos o n.º3 do artigo 12.º em que o prazo ordinário acrescido da prorrogação pode ter a duração de três meses (interpretação retirada da versão inglesa), enquanto que a versão portuguesa refere que "pode ser prorrogado até dois meses" – *cfr.* comentário 1º do artigo 12.º *In* "Comentário ao Regulamento Geral de Proteção de Dados", Edições Almedina S.A., 2018, de ALEXANDRE SOUSA PINHEIRO (et alia), pág. 340.

3.2.1. **Responsável pelo Tratamento**

Esta contraparte, a quem incumbe garantir a proteção dos direitos do titular deverá ser, nos dizeres da lei "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais."[204]– o Responsável pelo tratamento (em inglês, *controller*). No âmbito territorial, será aplicável a norma comunitária sempre que o Estabelecimento do Responsável[205] esteja situado na União, ainda que o tratamento dos dados ocorra dentro ou fora do território comunitário. Poderão estar, igualmente, incluídos nas obrigações emanadas pelo RGPD, os Responsáveis não estabelecidos na União que tratem sobre dados pessoais de titulares residentes no espaço comunitário (nos tramites do artigo 3.º nº2) ou no qual possa ser aplicável o Direito Comunitário por via do Direito Internacional Público. Nestes casos, o Responsável não estabelecido na União terá a obrigação de nomear, por escrito, um representante estabelecido na UE, excetuando-se os casos em que as operações de tratamento sejam ocasionais, não sejam abrangidos tratamentos em grande escala, sobre categorias especiais de dados (aos quais se inclui os dados relativos a condenações penais ou infrações) ou quando esse Responsável seja autoridade ou organismo público – Artigo 27.º RGPD.

O legislador comunitário harmoniza a consideração de quem deve ser enquadrado como contraparte juridicamente relevante do tratamento de dados pessoais, sendo aqueles sujeitos jurídicos que influenciam a esfera jurídica do titular dos dados, desde pessoas singulares a organismos diversos, com exclusão dos casos ilustrados no artigo 2.º nº2. Ultrapassando o perímetro da natureza jurídica coletiva, será Responsável pelo tratamento todas as pessoas singulares que efetuem operações de tratamento sobre dados pessoais de terceiros, desde que não advenham de atividades exclusivamente pessoais ou domésticas (artigo 2.º nº2 alínea c)). Importa ressalvar que a pessoa singular que venha a compartilhar dados pessoais de

[204] Definição do artigo 4.º ponto 7º, ao qual acresce ainda que, caso os meios de tratamento e finalidade sejam determinados pelo direito comunitário ou direito do Estado-Membro, os critérios aplicáveis a nomeação de responsável pelo tratamento poderá redigir-se nesse direito da União ou do Estado-Membro.

[205] Por interpretação do ponto 16 alínea a) do artigo 4.º, será estabelecimento principal (quando o Responsável detenha estabelecimentos em diferentes Estados-Membros) aquele em que estejam patentes as competências de projeção e execução das decisões sobre meios de tratamento e suas finalidades, o que poderá não coincidir com o estabelecimento onde se encontra a administração central. O mais usual é que o seja.

terceiros no espaço cibernético, a atividade deixará de se compor por mera conotação doméstica ou pessoal[206].

Via de análise, os tratamentos de dados pessoais terão o seu terreno de eleição nas relações jurídicas estabelecidas entre um titular de dados e uma pessoa coletiva, independentemente da sua dimensão[207], forma organizativa[208] ou atividade desenvolvida[209]. No caso de grupos de empresas (entre empresa central e filiais) há um enquadramento como sendo responsáveis pelo tratamento distintos[210], já que são entidade jurídicas com personalidade jurídica própria. Pode ainda suscitar casos em que o mesmo tratamento seja efetuado por mais do que um responsável e que, em conjunto, determinem as finalidades e os meios desse tratamento[211]. Serão designados por Responsáveis Conjuntos (artigo 26º), incumbindo a necessidade de estabelecer acordo que determine a quota-parte de responsabilidade de cada organização, tanto em aspetos de proteção e salvaguarda dos direitos e liberdades dos titulares dos dados, como no que concerne às obrigações para com os reguladores. Tal acordo deve refletir sobre as funções e relações dos responsáveis conjuntos e deve ser disponibilizado ao titular dos dados, com respeito pelos Princípios do Regulamento, sobretudo, o Princípio da Transparência. O titular dos dados poderá vir a exercer os seus direitos em relação a cada um dos responsáveis (número 3 do artigo 26.º)[212].

No contexto obrigacional, o Responsável ao ter as funções de controlo e administração dos dados, será aquele que se compromete, em consequência dessa qualificação, a cumprir as obrigações imposta por toda a legislação de proteção de dados. A lista de obrigações é vasta, nomeadamente: adoção de medidas de proteção de dados desde a conceção e por defeito (artigo 25.º); realização, quando aplicável, de registo das atividades de tratamento (artigo 30.º); cooperação com as autoridades de controlo (artigo 31.º); adoção de medidas

[206] A publicação de dados pessoais de índole pessoal/ familiar ou doméstico teve a sua clarificação no Tribunal Distrital de Gelderland (Holanda) no Processo nº C/05/368427 de 13 de maio de 2020 – no caso, a partilha de fotografias da neta nas redes sociais (Facebook), sem o devido consentimento dos representantes legais (autores), os mesmos que também partilhou fotografias noutra rede social (Pinterest). A Avó (réu) foi condenada à remoção das fotografias das redes sociais, à proibição de distribuir ou publicar outras fotografias da menor e, ainda, ao pagamento de uma coima no valor de 50.00€ por cada dia que não cumprir com a remoção da fotografia da menor (até limite máximo de 1000.00€), além do pagamento de uma coima de semelhante valor por cada dia que não cumprir com a remoção das fotografias dos autores na rede social Pinterest. É exemplo jurisprudencial que prova que atividades domésticas ou pessoais ficam despidas dessa exclusividade quando partilhas na Internet e, nesse sentido, sujeitam-se ao tratamento, nos termos do RGPD.
[207] Micro, pequenas, médias e grandes empresas, embora haja questões específicas no âmbito de grupos de empresas.
[208] Sociedades civis, sociedades comerciais, cooperativas, agrupamentos complementares de empresas, agrupamentos europeus de interesse económico, empresários em nome individual, entidades públicas, incluindo a Administração Pública.
[209] Atividades administrativas, agrícolas, comerciais, industriais, financeiras, artesanais, profissionais liberais ou prestações de serviços.
[210] Tal facto implicará a necessidade de uma base legal que permita a transferência de dados entre elas.
[211] Na prática, ocorre, sobretudo, quando uma base de dados é comumente partilhada a mais do que uma organização.
[212] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, *págs.* 73 a 75.

técnicas e organizativas para assegurar um nível de segurança adequado ao risco (artigo 32.º) as quais tiveram enfase no ponto 4. Medidas de Segurança (Capítulo 1) da presente dissertação; notificação a autoridade de controlo em caso de violação de dados pessoais (artigo 33.º); notificação ao titular dos dados acerca da violação de dados pessoais, quando ocorra nas circunstâncias enunciadas no artigo 34.º; realização de avaliações de impacto (artigo 35.º); proceder à consulta prévia, quando necessário (artigo 36.º); adotar códigos de conduta (artigo 40.º)[213] e procedimentos de certificação (artigo 42.º), quando implique a transferência internacional dos dados.

Esta listagem centra-se as obrigações de implementação e adequação das organizações ao disposto na legislação *data* protecionista, aspetos esses a desenvolver nos capítulos ulteriores. O facto é que deixamos, ainda, por referenciar obrigações imprescindíveis para iniciar uma visão de cumprimento com o disposto pelo legislador comunitário. Está em causa a primeira de todas as obrigações e a alteração fulcral do regulamento em comparação com a diretiva: ao Responsável pelo tratamento recai o Princípio da Responsabilidade – artigo 5.º nº2[214].

Nos termos da Diretiva, incumbia a cada autoridade a verificação e controlo sobre cada organização para comprovar que estaria a cumprir com as obrigações circundantes da proteção de dados. Com o Regulamento e a emanação do Princípio da Responsabilidade, há uma inversão do ónus da prova. Cabe agora a cada organismo uma autorregulação que garanta todos os Princípios relativos ao tratamento de dados pessoais constante, em termos gerais no número 1 desse mesmo artigo 5.º. Ademais, a Responsabilização implica não só a tomada de políticas adequadas (artigo 24.º nº2) e medidas regulatórias necessariamente eficazes para a mitigação de riscos que infrinjam nos direitos e liberdades dos titulares (artigo 24.º nº1), mas ainda na comprovação desse estado de *compliance,* melhor dizendo, na responsabilização pela efetividade da sua atuação[215]. E é neste espírito de estar, a todo o tempo, em condições de tal demonstração que é extremamente relevante o arquivo documental detalhado de cada atuação, isto é, a conservação dos registos de atividades por

[213] Em que se explicite as regras específicas de segurança de dados para cada segmento da entidade.
[214] *Cfr.* FILIPA MAGALHÃES e MARIA PEREIRA, *Regulamento Geral de Proteção de Dados – Manual Prático,* Vida Económica, 2018, *págs*. 35 a 39.
[215] Citemos o provérbio romano de Pompeia, Esposa de Júlio César: "À mulher de César não basta ser honesta, deve parecer honesta". O mesmo contexto é aplicado aos Responsáveis pelo tratamento aquando da entrada em vigor do Regulamento, já que, doravante, além das organizações terem a obrigação de estar em *compliance*, não basta estar nem parecer estar, implica comprovar que assim esteja.

parte do Responsável, com vista a provar essa mesma atitude de conformidade com o Regulamento e de cooperação com a Autoridade de Controlo – Considerandos nº 74 e 82 - ao que os anglo-saxões designam por *accountability*. Nesta via, voltemos a frisa a importância de implementar Sistemas de Gestão de Privacidade da Informação, no seguimento de linhas orientadores tais como a ISO 27001, 27002 e, sobretudo, a ISO 27701. Outras formas que reforçam o cumprimento deste Princípio seguirão, naturalmente, algumas obrigações *supra* listadas, desde o controlo prévio das operações planeadas (AIPD), à solicitação de consulta prévia às autoridades de controlo, mas, acima de todas, a criação do cargo de encarregado de proteção de dados.

3.2.2. **O Subcontratado**

Na larga maioria dos casos em que a relação jurídica de proteção de dados se suscita, não ficará apenas na esfera obrigacionista do organismo a quem venha determinar os meios e os fins do tratamento dos dados pessoais, já que não será a única entidade a lidar com os mesmos. Aliás, o processamento efetivo da informação pessoal tende a ser realizado através do subcontratado, por conta do responsável pelo tratamento. Consoante o artigo 4.º, no seu ponto 8, o subcontratado (denominado por *processor* na terminologia inglesa) é definido como "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*." A diferença para a corresponsável é que no caso de suscitar conjuntamente a responsabilidade perante o mesmo tratamento, aí as finalidades e meios de tratamento são decididos pelos Responsáveis conjuntos[216], estando a quota parte da responsabilidade definida no acordo. No caso da relação com o subcontratado, estamos perante uma figura que não poderá determinar as

[216] Na corresponsabilidade, o tratamento é efetuado por mais do que um responsável, aquando da determinação das finalidades e meios de tratamento, tornando a entidade corresponsável perante o titular de dados. Essa posição de Responsável Conjunto, nos tramites do artigo 26.º do RGPD, exigirá a elaboração de um acordo que determine a quota-parte de responsabilidade de cada organização. A forma jurídica do acordo dos corresponsáveis não é especificada pelo RGPD, mas nas linhas orientadoras 07/2020 do Comité Europeu para a Proteção de Dados, sobre os conceitos de Responsável e Subcontratado, fica esclarecido que tal acordo deverá seguir a forma de um documento vinculativo, como um contrato ou outro ato vinculativo ao abrigo da legislação da UE ou dos Estados-Membros a que os responsáveis pelo tratamento estejam sujeitos, desde que reflita, devidamente, as funções e relações entre os corresponsáveis, sendo que a essência desse acordo deve ser disponibilizada ao titular de dados. Podem surgir as corresponsabilidades que sigam a forma de participação conjunta devido a uma decisão comum, ou por propósitos convergentes, mas inseparáveis para a concretização das finalidades. O certo é que a qualificação da corresponsabilidade requer uma avaliação casuística para averiguar os critérios de "corresponsáveis por decisão comum versus corresponsáveis em resultado da convergência das decisões inseparáveis" que relevam para diferenciar as situações de Responsáveis Conjuntos e as situações em que são Responsáveis individuais/separados, sem vinculo associado entre eles, além das situações que envolvam um Responsável pelo tratamento com um ou mais subcontratados, uma vez que participam no desempenho do tratamento, mas realizam-no por conta do Responsável pelo tratamento.

finalidades e os meios do tratamento, caso contrário, tornar-se-ia responsável nesse tratamento e não apenas um mero subcontratado – vejamos no número 10 do artigo 29º.

A figura do subcontratado é clarificada pelo seu artigo 28.º, ou, melhor ainda, no Considerando n.º 81. Sucintamente, tendo em conta que é o próprio responsável pelo tratamento a determinar o subcontratado, haverá a necessidade de garantir que as atividades de tratamento sejam confiadas a subcontratados dotados de conhecimentos especializados e recursos para levar a cabo a execução das medidas técnicas e organizacionais e suficientemente capazes de cumprir com a segurança do tratamento (em concreto, com a concretização dos direitos do titular dos dados). Só através do recurso à subcontratação[217] com garantias suficientes para cumprir com o estado de conformidade é que é possível o Responsável ter bases que sustentam o cumprimento da sua Responsabilização. Um fator de indicação do cumprimento destes preceitos no momento da contratação do subcontratado será, em anexo à repartição de obrigações do acordo de subcontratação, alistar medidas técnicas e organizacionais que o subcontratado tende a aplicar na sua atividade laboral e, até a indicação de alguma formação associada ao RGPD, lecionada para os seus funcionários e colaboradores.

Na Diretiva 95/46/CE, aos subcontratados exigia-se, essencialmente, o cumprimento de deveres de segurança e confidencialidade, mas caberia ao responsável pelo tratamento assegurar a responsabilidade em caso de incumprimento, designadamente no que diz respeito aos titulares dos dados (artigo 23.º da Diretiva). Com a estrutura do Regulamento, acrescem deveres específicos ao ponto de levar à responsabilização do subcontratado em caso de incumprimento. A relação deixa de ter apenas efeito entre as partes, concedendo o direito aos titulares dos dados para agirem contra o subcontratado. Em concreto, alarga a sua esfera obrigacionista para o dever de aguardar pela instrução do responsável (artigo 29.º) o dever de registo das atividades de tratamento (artigo 30.º, nº2), o cumprimento da segurança no tratamento (artigo 32.º), além da nomeação de encarregado de proteção de dados (artigo 37.º). Torna-se indiscutível a Responsabilidade pelo incumprimento dos deveres específicos dirigidos aos subcontratados "*ou se não tiver seguido as instruções lícitas do responsável pelo*

[217] O subcontratado poderá, também ele, subcontratar o serviço (total ou parcialmente) desde que obtenha autorização por parte do responsável – artigo 28.º nº 2 e 4 do RGPD. Aqui sim parece-nos mais feliz a terminologia da tradução do Regulamento enquanto "subcontratante", porque o subcontratado, também veio a subcontratar, passe a redundância.

tratamento", nos termos do artigo 82.º, ficando, inclusive, sujeitos a aplicação de coimas enunciadas na redação do artigo 83.º.

Fica sublinhada essa responsabilidade pelo incumprimento quando o Regulamento, nos Considerandos nº 145 e 146, clarifica que podem ser intentadas ações, não só contra o Responsável, como também contra o Subcontratados. Tanto os responsáveis pelo tratamento como os seus subcontratados poderão vir a repartir, obrigatoriamente, os danos causados aos titulares por intermédio de tratamento que violem quer a norma comunitário, quer a de execução no direito dos Estados-Membros. Caso sejam envolvidos no mesmo tratamento causador de dados, a indemnização poderá ser repartida nos termos da Responsabilidade Solidária, por forma a que o titular tenha assegurada a indemnização integral que abarque os danos sofridos devido ao incumprimento (Considerando nº 146 *in fine*). Se o facto causador do dano não seja imputável a um destes sujeitos jurídicos, poderá, então, ver a sua responsabilidade exonerada, caindo sobre ele o ónus de prova. Salienta-se novamente, a importância do arquivo documental das atividades.

3.2.3. **Cláusulas da Subcontratação**

Quando o Responsável recorra aos serviços de um subcontratado, tal implicará a sua regulação por via de um contrato ou ato normativo que estabeleça "*o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias de dados pessoais*" além das obrigações específicas do subcontratado e, em contrapartida, dos direitos que façam parte da esfera jurídica do Responsável – artigo 28.º nº3. Deste contrato ou ato normativo sairá o preenchimento, por escrito[218] (artigo 28.º nº9), os requisitos formais do número 3 deste artigo, principalmente quanto ao compromisso da confidencialidade exigida, o tratamento dos dados pessoais, apenas mediante a instrução do Responsável, a adoção de medidas de segurança adequadas (a que remetemos para o ponto 4. Medidas de Segurança – Capítulo 1), a necessidade de autorização do Responsável caso o subcontratado queira se tornar subcontratante, o dever assistência perante o responsável "*para assegurar o cumprimento das obrigações decorrentes da realização de avaliações de impacto sobre a proteção de dados e da consulta prévia à autoridade de controlo.*"

[218] Por salvaguarda do Princípio da Transparência, o Responsável terá que disponibilizar o contrato caso o titular dos dados pessoais venha a requerer.

(Considerando nº. 95) e para fazer cumprir a obrigação de dar resposta a pedidos dos titulares de dados, além da necessidade de apagamento dos dados após a conclusão da prestação de serviços (excetuando os casos em que a sua conservação seja exigida) e de cooperação para efetivar as auditorias pertinentes.

A redação do contrato ou ato normativo deve seguir essas componentes podendo ter por base um contrato escrito, ou outro ato normativo desde que reduzido a escrito[219], no qual estejam repartidas as obrigações de cada interveniente - Acordo de subcontratação para efeitos do artigo 28.º do RGPD. O conteúdo do contrato plasmado no n.º 3 do artigo 28.º poderá ser preenchido através cláusulas contatuais-tipo estabelecidas pelo Comité Europeu para a Proteção de Dados[220] ou das cláusulas contratuais-tipo estabelecidas pela Comissão Europeia[221], nos termos dos n.ºs 7 e 8 do artigo 28.º. Nesta medida, o conteúdo do acordo garante a presença de obrigações especificadas do subcontratado com maior detalhe em relação às previstas na Diretiva.

Na prática, o acordo por vias contratuais pode desencadear algumas problemáticas: por um lado, os acordos de subcontratação assinados sem conhecimento da real dimensão do comprometimento, desencadeando, por vezes, a aquisição de certificações rápidas e formações definitivas (claramente falsa publicidade de "estar em conformidade de imediato e para sempre") por forma a demonstrar ao Responsável pelo tratamento um nível superficial de adequação em matéria de proteção de dados, processo esse que não tem outra forma de *compliance* se não a sua longevidade, quer para o entendimento e implementação, quer para a continuidade e pós adequação; por outro lado, para os subcontratados que tenham entendimento exato da dimensão (o que implica o reconhecimento das responsabilidades a que estão sujeitos), e que suscitam dificuldades no convencimento em assinar esses atos normativos, sobretudo, quando estamos perante temáticas como a *cloud computing* em que os mecanismos para processar os dados pessoais são difíceis de contornar e as entidades disponíveis a subcontratar no mercado são escassas[222].

[219] Cfr. n.ºs 3 e 9 do Artigo 28.º e considerando 81 do RGPD.

[220] Disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/dk_sa_standard_contractual_clauses_january_2020_pt.pdf.

[221] Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_pt.

[222] *Cfr.* NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, *pág*. 16.

Segundo TERESA VALE LOPES[223], "*A extensão das obrigações e responsabilidades do subcontratante, em conjunto com as pesadas sanções no âmbito do RGPD, são assim suscetíveis de gerar alterações na dinâmica de negociação dos contratos a celebrar entre os responsáveis pelo tratamento e subcontratantes, designadamente no que respeita à transferência de risco e ações de direito de regresso no caso do subcontratante ser sancionado devido a qualquer incumprimento por parte do responsável pelo tratamento*".

Por forma a aproximar à realidade empresarial mais comum no território português, isto é, as PME[224], verifica-se que o tratamento de dados pessoais relativos aos vencimentos, é efetuado por organização de contabilidade externa à qual se estabelece um acordo de Responsáveis conjuntos. Em relação a outras operações de dados pessoais realizadas por entidades externas, por via da subcontratação, será imprescindível articular cuidadosamente o artigo 28.º do RGPD, nomeadamente, no que diz respeito à celebração do acordo de subcontratação que cumpra os requisitos formais do n.º 3 do artigo 28.º e que tal redação seja revista periodicamente, por forma a refletir sobre elementos fulcrais a ter em conta. Exemplificativamente, deve ser requerida aquando da subcontratação, a cópia de políticas de segurança e de privacidade da entidade a subcontratar, de modo a verificar e documentar a fiabilidade e o conhecimento especializado na proteção de dados de tal entidade. Importa salvaguardar que, mais do que bem redigida, a subcontratação deverá ter efetividade prática, por forma a que o preenchimento de *compliance* das entidades envolvidas, não seja meramente teórico. Do ponto de vista técnico, é recomendável o uso de vias encriptadas e seguras para efetuar as comunicações entre estes sujeitos responsabilizados relativamente aos dados pessoais.

3.3. Autoridade de Controlo[225]

Sem menosprezar o papel preponderante das autoridades de controlo para que as disposições legais sobre a proteção de dados sejam concretizáveis, passemos a indicar breves

[223] No Artigo intitulado por "Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados", página 60, *in* Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2018, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf;

[224] PORTDATA – Base de Dados Portugal Contemporâneo (2016). "Pequenas e médias empresas em % do total de empresas: total e por dimensão". Disponível em https://www.pordata.pt/Portugal/Pequenas+e+m%C3%A9dias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimens%C3%A3o-2859 (consultável em julho de 2020).

[225] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, pág. 139.

reflexões do seu enquadramento na relação jurídica *data* protecionista e o paradigma nacional.

A autoridade de controlo é uma autoridade pública independente criada, obrigatoriamente, por cada Estado-Membro, consoante o artigo 51º do RGPD[226]. Enquanto reguladora perante o titular dos dados pessoais (caso este considere que os seus direitos tenham sido violados) e perante os tribunais (caso existam infrações penais associadas), o responsável incumpridor responde perante esta. Para isso, veste a sua caraterística distintiva de independência na prossecução das suas atribuições[227] e no exercício dos poderes[228] que lhe são conferidos. Os seus membros não solicitam, nem recebem instruções ou influências externas, cabendo a esses a impossibilidade de desempenhar outra atividade incompatível, mesmo que não remunerada. Estará intrínseca a missão de zelar pela fiscalização do RGPD, em prol dos direitos e liberdades fundamentais e a livre circulação dos dados pessoais, e contribuir para a coerente aplicação das normas *data* protecionista em cada Estado-Membro. Por forma a efetivar as suas atribuições, poderá a autoridade de controlo elaborar formulários de reclamação próprio, formulário de indicação do EPD, linhas orientadoras sobre temáticas em linha de conta socio-temporal[229] e que, para isso, o acesso será gratuito tanto para o titular como para o Encarregado de Proteção de dados, excetuando-se a possibilidade de aplicação de taxa de moderação nos casos de pedidos infundados reincidentes.

Quando uma autoridade de controlo verificar que se encontra perante um caso de tratamento transfronteiriço de dados[230], deverá informar a autoridade de controlo principal que, no prazo de 3 semanas decide se trata o caso consoante o artigo 60.º. Caso contrário caberá a resolução à autoridade de controlo inicial. Mas, por regra, caberá à autoridade de

[226] No ordenamento jurídico português, já prevista no artigo 35.º da CRP.
[227] Promover sensibilização e compreensão do público relativamente a riscos, regras e direitos associados ao tratamento, como também acerca das obrigações aos responsáveis e subcontratados; cooperar com autoridades de controlo de outros Estados-Membros; tratar as reclamações apresentadas pelo titular dos dados, investigar sobre o conteúdo da reclamação e informar do seu resultado, num prazo razoável – artigo 80.º; elaborar cláusulas contratuais-tipo para os termos do artigo 28.º nº8 e 46.º nº2 alínea d); elaborar lista de operações que exijam a realização de uma AIPD, nos termos do artigo 35.º nº4; orientar sobre operações de tratamento, nos termos do artigo 36.º; conservar registos internos de violações do RGPD e das medidas tomadas, nos termos do artigo 58.º nº2; entre outras atribuições, ilustrativamente consultáveis no artigo 57.º do RGPD.
[228] Poderes de investigação, de correção, consultivos e de autorização, todos redigidos detalhadamente no artigo 58.º do RGPD.
[229] Factos novos relevantes com incidência na proteção de dados pessoais.
[230] Com auxílio da definição do ponto 23 do artigo 4.º, o tratamento transfronteiriço de dados pode ocorrer quando o Responsável ou subcontratado esteja estabelecido em mais do que um Estado-Membro e, por isso o tratamento tenha de ocorrem em Estados Comunitários distintos, colocando em mesa, pelo menos, duas autoridades de controlo. Além disto, poderá ocorrer quando "*afeta substancialmente, ou é suscetível de afetar substancialmente"* os titulares residentes de Estados-Membros distintos. Interprete-se no sentido de deter caraterísticas que possam causar danos ou prejuízos a terceiros em situações que ultrapassam o critério da normalidade aquando do tratamento de dados. – Orientações do GT 29 (WP 244 ver.01) *Orientações sobre a Identificação da Autoridade de Controlo Principal do responsável pelo Tratamento ou do subcontratante.* Versão portuguesa do documento disponível em: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf (consultável em janeiro de 2021).

controlo principal, após "remessa", a responsabilidade de gestão das operações do tratamento transfronteiriço em causa e a coordenação de investigações em cooperação com as autoridades interessadas, isto é, aquelas que também tenham sido afetadas pelo tratamento de dados pessoais e que tenha competência para o investigar (artigo 4.º ponto 22). A autoridade de controlo principal suscita-se em nome do Princípio do balcão único e da coerência na fiscalização e investigação de operações de tratamento de dados pessoais.

Para a identificação da autoridade de controlo principal, as orientações do Grupo de Trabalho 29 (WP 244 rev.01) indica que dependerá se estamos perante o tratamento por via do responsável ou o tratamento diretamente imputável ao subcontratado[231]. A identificação da ACP relativamente ao Responsável será a do país onde estará localizado o estabelecimento principal da organização – artigo 56.º. O problema surge quando a organização seja, por exemplo, multinacional, com vários estabelecimentos. O critério a seguir será o local onde é concedida a aprovação final das decisões sobre as finalidades e os meios de tratamento (poderá não ser semelhante ao local onde se encontra instalada a administração central)[232]. Se por acaso as decisões sejam tomadas em diferentes estabelecimentos, haverá mais do que uma autoridade principal, mas apenas relevante o local do estabelecimento onde foram tomadas as decisões sobre o tratamento transfronteiriço em causa. A identificação relativamente aos subcontratados será o do seu estabelecimento principal, equivalente à sua administração central ou, na sua inexistência, será onde sejam exercidas as principais atividades do tratamento – alínea b) do ponto 16 do artigo 4.º[233].

Afigura-se essencial que as empresas centralizem a competência para executar decisões em um único Estado-Membro, já que é essencial a identificação de forma precisa do seu estabelecimento principal. *A contrario* poderá gerar uma incerteza relativa a que autoridade de controlo a organização esteja efetivamente sujeito e não beneficie, de forma clarificada, do sistema do balcão único. Seguir-se-iam implicações devido à incerteza de qual a autoridade de controlo estará a organização sujeita a responder no que respeita a obrigações diretas para efeitos de conformidade com o RGPD (de designação do EPD, de solicitação de pareceres ou

[231] Nos casos em que implique ambos os sujeitos jurídicos, a autoridade principal competente será a do responsável pelo tratamento, ficando a do subcontratado como autoridade de controlo interessada e, dessa forma, também participativa no processo de cooperação – Considerando n.º 36.
[232] Poderá ainda auxiliar a identificação do local de estabelecimento principal outros aspetos de logística como o local onde se encontra a "empresa-mãe", onde se situe o diretor com responsabilidades globais de gestão do tratamento transfronteiriço, *et cetera*.
[233] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 149 e 150.

de consulta prévia a autoridade verdadeiramente competente). Todavia, poderá ser alarmante o facto das autoridades de controlo com histórico reduzido de coimas aplicadas, ser um fator essencial para as grandes empresas adaptarem o seu estabelecimento principal naquele Estado-Membro ao qual aquela Autoridade terá a sua competência.

O facto da supervisão ou autorização prévias da Autoridade de Controlo não serem exigíveis além do plasmado no RGPD, trouxe consigo um regime de atuação mais reativo do que preventivo, o que, na prática, certas implicações para a efetiva proteção dos dados pessoais, ainda que, pelo lado positivo, venha afastar burocracias administrativas e temporais quando seja necessário iniciar uma atividade que requeira o tratamento de dados pessoais. Isto é, ainda que se faça circular dados indispensáveis para o mercado interno com menos burocracia, a proteção do titular, deixada à atuação reativa, poderá dar azo a dificuldade na sua efetivação, especialmente quando as autoridades de controlo não sejam dotadas de recursos humanos suficientes.

Nos parâmetros nacionais, o caráter independente, as atribuições e poderes da autoridade de controlo são desempenhados pela Comissão Nacional de Proteção de Dados (CNPD), legalmente considerada como Autoridade de Controlo Nacional pelo artigo 3.º da Lei n.º 58/2019, diploma legal esse que veio alterar no seu artigo 63.º, algumas disposições legais da Lei de Organização e Funcionamento da Comissão Nacional de Proteção de dados[234]. Ressalva-se que o seu caráter independência, com autonomia administrativa e financeira, é reforçado no artigo 4.º nº1, 3 e 4 da LNE.

4. Encarregado de Proteção de Dados

Após uma análise conceptual extensiva, podemos reconhecer que a larga maioria dos organismos e entidades ficam sujeitos ao disposto na legislação sobre a proteção de dados e que, na presença de um estado de incumprimento, cada organização será sujeita a medidas corretivas capazes de levar ao colapso, não só por via das elevadas coimas aplicáveis pela autoridade de controlo, mas ainda pela possível sujeição a indemnizar diretamente os titulares dos dados pelos danos causados.

[234] Lei n.º43/2004, de 18 de agosto, alterada pela Lei n.º 55-A/2020, de 31 de dezembro.

Assim sendo, afigura-se pertinente que as organizações tenham dado por concluído todo o processo de implementação, e que estejam cientes da relevância da pós-adequação. São dois ciclos distintos: o primeiro de adaptação e implementação das obrigações que advêm deste "novo" regulamento; o segundo de constante adequação dos procedimentos necessários para a defesa dos direitos e liberdades do titular dos dados, aspetos que exige uma atuação direta dos auditores de privacidade e, mais do que nunca, o desempenho da figura fulcral para que a organização se considere em conformidade com o Regulamento – o *Data Protection Officer*.

Ao EPD compete desempenhar um papel que garanta que a organização cumpra todas as obrigações legais imputadas pelo Regulamento, não só para o acompanhamento da implementação das medidas e alterações necessárias ao alcance do ponto de compliance inicial como também para a posterior regulação e fiscalização interna sucessiva. Na relação jurídica retratada no Capítulo anterior, o Encarregado de Proteção de Dados estará no centro de todos os elementos, sendo não só o consultor acessível para cada titular de dados pessoais[235], como também a ponte para o contacto entre o Responsável pelo tratamento pertencente à organização e a autoridade de controlo nacional com competência territorial. É um intermédio, muito similar à figura de mediador, entre as várias figuras com as quais a organização tenha que lidar, quer para a autoridade de controlo quer para a vasta possibilidade de titulares de dados pessoais sujeitos ao tratamento dessa organização – clientes, fornecedores, trabalhadores, parceiros, gestores, entre outros. O seu fulcro inigualável é, sem dúvida, o indício mor da *compliance*, até porque em alguns casos, como analisaremos *infra*, a sua nomeação é de obrigatoriedade intransponível.

Sublinhe-se que tal cargo assume um "*papel fundamental na promoção de uma cultura de compliance na área de proteção de dados dentro da organização para a qual trabalha"*[236].

Historicamente, o Encarregado não tem a sua origem plena no RGPD, embora se reconhece que o espírito que o circunda seja inovador na atual letra da lei. O contacto primário com esta figura surgiu, no contexto da legislação da proteção de dados pela Diretiva

[235] Consoante as orientações do GT 29 (WP 243 ver.01), é recomendável que o Encarregado de Proteção de Dados esteja localizado na União Europeia, a menos que possa exercer as suas funções de forma mais eficiente se estiver situado fora da União (o que poderá ocorrer no caso do Responsável pelo tratamento ou o subcontratado estarem estabelecidos fora do território comunitário).
[236] No Artigo de TERESA VALE LOPES, intitulado por "Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados", página 67, *in* Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2018, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf

95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro, efetivamente plasmado no seu Considerando nº 54, bem como no n.º2 do artigo 18.º e no n.º2 do artigo 20.º. Na redação da Diretiva, o EPD estaria apenas relacionado com a tarefa de controlo prévio à realização de tratamentos com riscos particulares, por forma a cooperar com a Autoridade de controlo. Nesta época a sua nomeação era puramente voluntária[237], deixando na tomada de decisão de cada entidade, mas a sua existência no seio organizacional era fundamento necessário para que o Responsável beneficiasse da isenção da notificação obrigatória antes de serem realizados tratamentos, particularmente, de risco – artigo 18 nº1 e nº2 da Diretiva. Com o aparecimento do Regulamento[238], o diploma faz exaltar o papel do DPO no novo sistema de gestão e governação da privacidade[239].

Criou-se a figura intitulada de *Data Protection Officer* (DPO) ou *Chief Privacy Officer* (CPO) que em tradução para a Língua Portuguesa, denomina-se por Encarregado de Proteção de Dados. Uma tradução direta, em parte, infeliz. Pode, de facto, estar encarregue de assegurar que direitos e liberdades dos titulares de dados não sejam suscetíveis de virem a ser prejudicados pelas operações de tratamento, quando tratados consoante as orientações, recursos e mecanismos mais recomendados tendo em conta a tecnologia disponível. Mas o certo é que, da sua atuação, o EPD nunca será pessoalmente responsável nos casos de incumprimento das normas do Regulamento (daí o termo "encarregado" sem qualquer veste de Responsabilidade ser razoavelmente questionável). Tal margem de responsabilidade fica claramente centrada na esfera jurídica do responsável pelo tratamento ou subcontratado, estando obrigado, como *supra* analisado, à comprovação da conformidade (artigo 24.º nº1).

Ademais, fica a cargo da organização a obrigação de assegurar que o DPO dispõe dos recursos necessários ao desempenho das suas funções, estando numa posição de total independência sem que possa, por isso mesmo, acumular cargos que coloquem em causa essa vertente. O que não é impeditivo de vir a exercer outras funções dentro e fora da organização.

[237] A transposição da prática de nomeação do EPD surgiu apenas nos normativos de França, da Suécia, da Holanda, da Alemanha e do Luxemburgo, pelo que o ordenamento jurídico português não teve, até a LNE que transpôs o RGPD, qualquer contacto com esta figura.
[238] O Regulamento bebeu inspiração na lei alemã – Lei Federal Alemã de Proteção de dados *(Bundesdatenschutzgesetz – BDSG)* – que já imponha obrigatoriamente a nomeação de um encarregado de proteção de dados às entidades detentoras de, pelo menos, 20 trabalhadores que procedessem ao tratamento não automatizado de dados ou, pelo menos, 9 que trabalhassem em tratamento automatizado de dados. Na lei alemã, a Encarregado deveria ser um profissional altamente qualificado na matéria de proteção de dados e estaria protegido em caso de despedimento coletivo, exceto se incumprisse gravemente nos seus deveres.
[239] *Cfr.* ANA FAZENDEIRO, *Regulamento Geral sobre a Proteção de dados*, Almedina, 3ª edição, 2018 *págs.* 19 a 25.

Até na própria estrutura do texto normativo, releva o facto da sua regulamentação ter sido redigida no Capítulo IV do RGPD "Responsável pelo tratamento e subcontratante", cercado de pilares base do estado pleno de conformidade, designadamente a "Segurança dos dados pessoais" da qual faz parte a notificação aquando da violação de dados pessoais, além da seção da "Avaliação de impacto sobre a proteção de dados e consulta prévia" e dos "Códigos de conduta e certificação".

4.1. Nomeação Obrigatória ou Facultativa

Nos termos do artigo 37.º do Regulamento, o responsável pelo tratamento e o subcontratado têm a obrigação de nomear um encarregado de proteção de dados sempre que estiver preenchidas alguma das três situações alistadas[240].

Respeitando a exposição redigida, sempre que "*o tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional*[241]". A designação por "autoridade ou organismo público" não é produzida no diploma comunitário, por forma a deixar essa caraterização nas mãos do legislador nacional. Será, portanto, no sentido comum de que autoridades nacionais, locais ou regionais, além de toda a panóplia de organismos públicos que desempenham funções de serviço público e de exercício da autoridade pública. Por análise ao n.º1 e 2 do artigo 12.º da Lei n.º58/2019, são entendidas por "entidades públicas" todas as que façam parte do sentido comum *supra* perspetivado, ao que se pode incluir pessoas singulares ou coletivas de direito público ou privado nos diversos setores que as tornem beneficiarias do estatuto utilidade pública, o que incluiria os órgãos reguladores de profissões (caso das Ordens, em Portugal)[242]. Isto implica que por cada ministério/ área governativa, por cada secretaria regional, no caso das regiões autónomas, por cada município, incumbindo à câmara municipal, por cada freguesia com mais de 750 habitantes, incumbindo à junta de freguesia e por cada restante entidade da qual entre

[240] Saliente-se que pode ser exigida a designação noutras situações ilustradas no artigo 37.º nº4.
[241] Advém do exposto na Diretiva (UE) 2016/680, artigo 32.º. Não implica que os tribunais e demais autoridades judiciais tenham, na sua totalidade, a isenção de nomear obrigatoriamente um EPD. Se tiver em causa um bar concessionado ou máquinas de *vending*, não estarão retirados da obrigação que possa preencher nas alíneas b) e c) do artigo 37.º nº1 do RGPD.
[242] Nos termos das Orientações emanada pelo Grupo de Trabalho do artigo 29º, estes casos ficam enquadrados nesta obrigação por esta via, devido ao facto dos titulares estarem similarmente condicionados ao tratamento dos seus dados pessoais tendo pouco ou nenhum poder de decisão e que a designação obrigatória virá como proteção adicional nesta circunstância em que o titular é notoriamente parte fraca da relação jurídica.

nesta panóplia, é necessário a nomeação de "pelo menos" um encarregado de proteção de dados.

No mesmo artigo 12.º da LNE, e por respeito ao artigo 37.º nº3 do RGPD, ficam abertas as hipóteses de designar mais do que um encarregado para a mesma autoridade pública (já que contempla a expressão de "pelo menos um"), como ainda de designar o mesmo encarregado para desempenhar as funções em mais do que uma entidade pública, não sendo obrigatório o exercício de funções em regime de exclusividade (números 4º e 5º do artigo 12.º), ressalvando ainda que em caso de ser nomeado para desempenhar funções numa entidade com atribuições de controlo e regulação, claro está, não poderá ser designado, em simultânea, para desempenhar funções com a entidade sujeita ao controlo (artigo 12.º nº6 LNE).

Para CRISTINA PIMENTA COELHO, "(…) *não se afigura admissível que um ministério nomeie um único encarregado de proteção de dados, independentemente da natureza e volume dos dados pessoais que trata e do número de titulares de dados envolvidos, sob pena de o DPO não poder desempenhar cabalmente as suas funções"*[243]. Nesta matéria o Regulamento exige que, quando seja designado um único DPO para várias autoridades ou organismos, que se "tenha em conta a respetiva estrutura organizacional e dimensão" (*cfr.* n.º3 do artigo 37.º do RGPD). Portanto, não nos parece ilícita a partilha do mesmo DPO por vários serviços públicos, independentemente da dimensão, desde que seja tinha em conta uma correta rede de interlocutores com Encarregado-Geral, uma equipa multidisciplinar e com conhecimento específico na matéria que permita garantir a acessibilidade com esse Encarregado-Geral, em consonância com a sua dimensão. Em conclusão ao refletido, mais do que questionar a designação de um Encarregado-Geral para diversos serviços públicos, relevará averiguar se a sua acessibilidade é posta em causa. Desde que contenha uma rede adequada e proporcional de colaboradores diretamente associados aos serviços públicos, poderá haver a possibilidade de desempenhar as suas funções, pelo que deverá ser uma questão analisada casuisticamente.

[243] *In* "Comentário ao Regulamento Geral de Proteção de Dados", Edições Almedina S.A., 2018, de ALEXANDRE SOUSA PINHEIRO (et alia), pág. 470.

Noutra situação, no âmbito das entidades privadas[244], o artigo 37.º nº1 alíneas a) e b)[245], estabelece ainda a obrigatoriedade de nomeação do DPO sempre que: primeiro, *"As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala";* segundo, quando essas atividades principais "*consistam em operações de tratamento em grande escala de categorias especiais de dados (…)*[246] e *de dados relacionados com condenações penais e infrações(…)"*.

São nestas expressões ambíguas que nos socorremos através das orientações do GT 29 "WP243 rev.01". A expressão "atividade principal" será aquela que seja fundamental para o desenvolvimento da atividade, mas não a razão de ser dessa atividade, isto é, todas as atividades essenciais para o alcance de objetivos do responsável pelo tratamento designadamente as atividades primárias e não auxiliares (às quais ficam excluídas as auxiliares, por aplicação do Considerando nº 97). No contexto prática, tomemos o exemplo do GT 29 quanto aos hospitais, em que atividade principal é a de prestar cuidados de saúde, mas que tal engloba uma parte indissociável de operações necessárias à prossecução da prestação de cuidados hospitalares, entre elas, os registos de saúde dos utentes. Já nos estabelecimentos de ensino a atividade principal é a de dar formação, pelo que estará indissociavelmente ligada a operações de tratamento de dados pessoais, nomeadamente, avaliações dos alunos ou dados pessoais simples dos professores, colaboradores e funcionários.

Já a existência de um "controlo regular e sistemático" implica que esteja em causa um controlo[247] recorrente, contínuo e constante (ou seja, regular), mas também predefinido/ metódico tal como ocorre num sistema (isto é, sistemático). Em termos práticos, o critério fica certamente preenchido quando estejam perante atividades associadas ao intoxicante marketing digital, explorações de redes de telecomunicações, publicidade comportamental,

[244] Grupos empresariais podem, da mesma forma que as autoridades públicas, nomear um único encarregado de proteção de dados para desempenhar as funções, desde que esteja acessível para cada estabelecimento e que não desempenhe funções, internas ou externas, conflituantes com o seu papel perante o Regulamento – número 2 do artigo 37.º RGPD.

[245] Alíneas transpostas na íntegra para o artigo 13.º da LNE.

[246] O GT 29 elucida que apesar da conjunção "e" estar no artigo, o texto deve ser interpretado como significando "ou", não havendo nenhuma razão estratégica para exigir, cumulativamente, os dois critérios. A existência de um deles já é suficiente para alargar o risco no tratamento dos dados pessoais.

[247] Podemos retirar parte da interpretação através do que o legislador comunitário considera como "controlo dos comportamentos dos titulares de dados" no Considerando nº24, mas a título meramente exemplificativo. O controlo nos termos do artigo 37.º nº1 alínea b) não se cingirá apenas a formas de seguimento e definição de perfis do titular no ambiente cibernético. A geo localização do trabalhador poderá, certamente, preencher o critério de controlo regular e sistemática e, por esse modo, definir a obrigação de designar um EPD.

definição de perfis, entre outros. Chamada de atenção, em particular, aos dispositivos conectados em linha (alvo de análise individual na nota de rodapé nº 62), por exemplo, nas organizações que captam dados através de automóveis inteligentes, domótica, contadores inteligentes, entre outros.

Todavia, a interpretação continuaria ambígua se não tivéssemos ciente o significado de operações de tratamento "em grande escala". Este é critério necessário para que qualquer entidade privada veja as suas obrigações alargadas para a nomeação do EPD, tal é presença do termo nas duas alíneas associáveis no artigo 37 º. É um conceito ao qual a interpretação deve ser guiada pelas linhas orientadoras do Considerando nº91[248]: "*visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, (e que) possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco"*.

O GT 29 recomenda, essencialmente, que sejam tomados em consideração diversos fatores para determinar se o tratamento é efetuado em "grande escala", designadamente, o número de titulares de dados afetados (numérico ou percentual *per capita*), o âmbito geográfico da atividade de tratamento, a duração ou permanência da operação, o volume de dados e alcance dos diferentes elementos de dados objeto de tratamento. Está claro que a verificação necessitará de uma consulta extensa sobre informações contextuais da organização, impulsionando o melhor conhecimento da estrutura, operacionalidade e disposição internas. Será tratamento de grande escala todo o tratamento de dados no exercício das atividades hospitalares (como o próprio considerando 91 auxilia na interpretação), o tratamento de dados num sistema de transportes públicos, o tratamento de dados pessoais para finalidades publicitárias comportamentais efetuada por um motor de busca, tratamento no exercício de atividade normal de companhias de seguros ou de banco, *et cetera*.

O problema coloca-se na zona cinzenta das operações, em que não se terá a noção de que são praticadas operações de tratamento em grande escala com interpretação dos critérios de demográficos (tratamento de dados pessoais de um número significativo de cidadãos, atendendo à densidade populacional e um território), como ocorre no âmbito de PME. Mais

[248] Não será aplicável nas mesmas modalidades posto que o considerando tem em linha de conta elementos específicos do contacto de Avaliação do Impacto sobre a proteção de dados.

fácil será verificar a carência de tal nomeação numa empresa ou organização com operações de tratamento decorrentes de uma base de dados significativa, independentemente de ter muitos ou poucos funcionários.

Em suma, no domínio das entidades privadas, nem sempre fica evidente que a organização esteja ou não obrigada a nomear um DPO, mesmo após uma eficiente e extensiva análise interna. Por salvaguarda do Princípio da Responsabilidade imposto tanto no *controller*, como no *processor*, no caso em que estejam perante a zona ambígua de determinação obrigatória do EPD, em que a decisão da contratação de um EPD resulte da interpretação efetuada pelo responsável do tratamento, afigura-se imprescindível efetuar o arquivo documental da análise interna que leve à conclusão da não nomeação do DPO, por forma a comprovar que foram adequadamente tomados em consideração os fatores enunciados no artigo 37.º. Caberá aos auditores avaliar a opção tomada pelo Responsável ou subcontratado e recomendar procedimentos diferentes, caso discordem dessa tomada de decisão[249].

Para as organizações que entendam conveniente designar um EPD a título voluntário, após a sua nomeação estarão igualmente sujeitas aos requisitos de nomeação, posição e atribuições dos artigos 37.º a 39.º.

Há a possibilidade de o Encarregado nomeado pertencer à organização (desde que não coloque em causa a proibição de exercer funções conflituantes[250]) ou que seja externo (como profissional liberal). Na primeira opção, ainda que possa gerar problemas laborais quando as funções de DPO cumulem com funções originárias (carecendo de delimitação dos contornos, por forma a comprovar que não hajam funções conflituantes), será uma vantagem quando a nomeação fique preenchida com quem tenha conhecimento amplo sobre a atividade do responsável pelo tratamento e que tenha maior prontidão em manifestar uma opinião crítica sobre os processos de tratamento que decorram na entidade. Na opção externa, embora fique dificultada a perspetiva do DPO enquanto membro da organização, este dificilmente receberá instruções relativamente ao exercício das suas funções. Outro aspeto a destacar é que, não sendo possível a sua destituição nem penalização pelo responsável pelo tratamento ou pelo

[249] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 93 a 95.

[250] Não existe uma listagem taxativa de cargos não cumuláveis com o de EPD, mas podemos exemplificar que gerará incompatibilidades com as funções de advogado da entidade, diretor ou administrador por departamentos de recursos humanos, de informática, de *marketing*, de logística ou de contabilidade, e, naturalmente, o cargo de Responsável pelo tratamento.

subcontratado pelo facto de exercer as suas funções, quando ocorra a nomeação de um elemento interno e que cumule com outras funções originários, tal facto dificultará a apreciação sobre a forma como atuou: se como DPO e, assim sendo, não permite a sua penalização; se por intermédio das funções originárias que abrem caminho a penalização.

Em matéria de designação de um DPO externo, CRISTINA PIMENTA COELHO no 9º comentário ao artigo 38.º[251] considera se o facto dos advogados exercerem funções de DPO cumulativamente com o exercício de funções de consulta jurídica e de patrocínio judiciário, se levanta a incompatibilidade, sobre o qual conclui que será "(…) *mais razoável considerar existir incompatibilidade apenas no contexto de processos relacionados com a proteção de dados ou com matéria atinentes ao RGPD."* (à semelhança da última posição assumida pelo Conselho dos Advogados Europeus – CCBE) e que "*Nos demais casos, o advogado que também exerça ou que tenha exercido as funções de DPO deverá avaliar se existe ou não impedimento e abster-se de praticar atos profissional cujo exercício possa suscitar, em concreto, uma incompatibilidade*".

De facto, nos termos do artigo 82.º do Estatuto da Ordem dos Advogados (EOA), aprovado pela Lei n.º 145/2015, de 9 de setembro, não se prevê incompatibilidade do exercício da advocacia com as funções de DPO, mas ao ser DPO de uma entidade, será impeditivo de assumir o mandato forense em processos relacionados com o tratamento de dados dessa mesma organização, envolvendo conflito de interesses (*cfr.* artigo 83.º do EOA). Sublinhe-se, ainda, a recomendação adotada pelo Conselho Geral da Ordem dos Advogados, em sessão plenária de 28 de setembro de 2018 de que "Nos termos do disposto no artigo 83.º, 1, 2 e 6, do Estatuto da Ordem dos Advogados, os advogados estão impedidos de exercer a advocacia e, assim, impedidos de exercer o mandato forense ou a consulta jurídica, para entidades para quem exerçam, ou tenham exercido as funções de Encarregado de Proteção de Dados".

Independentemente da opção, importará ter em conta os seguintes aspetos genéricos: a designação desta figura deveria ser levada na implementação inicial do regulamento; implica uma fundamentação perspicaz sobre a opção que seja tomada; caso seja criada, obrigatória ou voluntariamente, esta figura, o Responsável tem a obrigação de disponibilizar os

[251] *In* "Comentário ao Regulamento Geral de Proteção de Dados", Edições Almedina S.A., 2018, de ALEXANDRE SOUSA PINHEIRO (et alia), pág. 477.

recursos[252] financeiros, instalações, equipamentos e pessoal necessários[253] ao desempenho das funções; por último, a não verificação da designação do EPD ou o desrespeito pelos direitos que lhe pertencem, abrir lugar à desconformidade com o Regulamento e à aplicação de coimas avultadas[254].

4.2. Posicionamento, Direitos e Obrigações do DPO

Segundo o exposto até então, o Responsável pelo tratamento ou o Subcontratado deve ponderar acerca da existência de um Encarregado como uma vantagem (e não pelo lado de custos acrescidos que acarreta à organização). A existência desta figura no seio organizacional, a que exige a composição da equipa do DPO com elementos focados exclusivamente na salvaguarda dos direitos *data* protecionistas[255], será um fator extra de confiança para futura clientela, colaboradores e funcionários. Além do mais, ao ser dotada de elementos profissionalmente enquadrados na temática de proteção de dados, levará ao preenchimento de linhas orientadoras de *compliance* (procedimentos contextualizados).

Melhor ainda, se voltarmos ao tema de implementação do Sistema de Gestão da Privacidade da Informação (ISO 27701), isto é, boas práticas que complementam as exigências do Regulamento, sabemos que é particularmente impossível vir a ser concretizada sem que venha a alcançar um Sistema de Gestão da Segurança da Informação (ISO 27001 e ISO 27002). A reflexão é que o DPO que venha a concretizar as práticas associadas à privacidade e aos dados pessoais, virá, por acréscimo, a concretizar as linhas orientadoras internacionalmente recomendáveis de todo o sistema de informação e não apenas dos dados pessoais,

[252] A CNPD, no Parecer n.º 20/2018 (Processo n.º6275/ 2018), concretamente na página 6v. sobre a Proposta de Lei n.º 120/XIII/3.ª, reforça a obrigação do Responsável em "fornecer ao encarregado de proteção de dados os recursos necessários para o desempenho das suas funções e a *manutenção dos seus conhecimentos"* (artigo 38.º nº2 RGPD), vindo, por isso, a contestar, entre outros, o artigo 6.º nº1 alínea g) da Proposta de Lei em que alargava as atribuições imputadas à CNPD, considerando da competência da Autoridade de controlo o "*promover ações de formação adequadas e regulares destinadas aos encarregados de proteção de dados*". Considerou que tal redação transferia o ónus formativo para a autoridade de controlo, efetuando uma clara subversão das regras. Esta norma foi removida do articulado e caberá ao Responsável disponibilizar ações formativas e de sensibilização ao EPD que nomeie. Uma remoção infeliz, já que, por remissão às linhas orientadoras do GT 29 em análise, "é igualmente conveniente que as autoridades de controlo promovam formações adequadas e regulares destinadas aos EPD".

[253] Há quem entenda que deve ser criado o responsável da proteção de dados (figura não expressamente consagrada no RGPD) que servirá como ponto de contacto entre o responsável pelo tratamento e o EPD (ao qual se inclui uma equipa multifacetada que se afigure necessária, sobretudo nos casos de empresas multinacionais ou de encarregados que sejam nomeados para vários setores públicos), tendo funções de cooperação – *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs *88 a 91.*

[254] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 95 a 98.

[255] Normalmente composta por técnicos de gestão, informáticos e juristas.

salvaguardando dados confidenciais[256] associados à entidade e que não veste a proteção do regulamento. Ou seja, estamos perante um Programa de "win-win" já que as organizações ficam em posição comprovadora do estado de conformidade (quanto aos profissionais qualificados), desde que venha a utilizar padronizações internacionalmente reconhecidos como procedimentos adequados (além de salvaguardar adequadamente dados importantes da Pessoa Coletiva), e os titulares que vêm os seus direitos ressalvados pela melhor atuação possível. Poderíamos ainda falar num "ganho triplo" no caso da contratação de auditores externos que passam a ampliar o seu mercado de serviços a prestar.

4.2.1. **Caráter, Posicionamento e Funções a Desempenhar[257]**

Nos termos do artigo 37.º nº5, o Encarregado de Proteção de Dados "é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar funções referidas no artigo 39.º". Tal redação deixa a critério[258] dos Estados-Membro o nível de especialização e competências a ser preenchido para que seja legitima a sua escolha. No âmbito nacional, como era já expectável, exige que a designação siga os requisitos abstratos do nº5 do artigo 37.º do RGPD, sem carecer de certificação profissional – artigo 9.º nº1 da LNE. É uma redação, do ponto de vista prático, infeliz que deixa à organização a designação arbitrária de quem venha a desempenhar esta função. Talvez seja um reconhecimento do estado prolongado de escassa capacidade financeira para investir num profissional minimamente qualificado, aspeto reforçado em época pandémica.

Vejamos, por base na interpretação recomendada pelo GT 29, os requisitos de especialização do artigo 37.º nº5 do Regulamento dependem, logicamente, da atividade de tratamento ser mais ou menos complexa. A designação será de forma rigorosa no âmbito de organizações que esteja em constante transferência de dados pessoais para fora da União Europeia ou se estiver em causa um tratamento de grandes quantidades de dados sensíveis. Nos restantes casos a designação quanto às competências, será com base em critérios de

[256] Receitas secretas, projetos sem registo de propriedade intelectual, conhecimentos que fazem a entidade se destacar de todas as outras no mesmo setor (quais os pormenores dos produtos ou serviços que tendem a garantir o êxito à exposição para a clientela, *et cetera*).
[257] *Cfr*. NUNO SALDANHA, *Novo Regulamento Geral de Proteção de Dados – O que é? A quem se aplica? Como implementar?,* FCA, 2018, págs. 117 a 119,
[258] Desde que a designação tenha por base as suas "qualidades profissionais" e "conhecimentos especializados" em matéria *data* protecionista, embora sejam critérios abstratos, de difícil contestação prática.

sensibilidade e de necessidade, desde que preencha atributos pertinentes de domínio das legislações, das práticas internacionalmente reconhecidas (às quais se incluem as ISO 27001, 27002 e ISO 27701) e de conhecimento profundo do RGPD. Ora, por reflexão dos seus efeitos práticos, se uma organização vier a designar um funcionário interno para desempenhar esta figura, sem que tenha o nível adequado de especialização e competências (sem falar de casos em que possa desempenhar funções conflituantes, consoante o número 6 do artigo 38.º do RGPD), terá, atualmente, a CNPD a competência para investigação e aplicação de coimas por não estar preenchida a designação adequada?

Segundo consta da base de dados que apresenta as coimas aplicadas após a entrada em vigor do RGPD (disponibilizada pela Sociedade Internacional de Advogados "*CMS Law Tax*" por via do "*GDPR Enforcement Tracker"*[259]*)* em Portugal, não surgiu, desde então, qualquer sanção por incumprimento de nomeação do DPO, o que denota alguma leveza oriunda da Comissão Nacional[260]. Sob consulta do Relatório de Atividades de 2017/2018 da CNPD[261], a maior parte das coimas aplicadas surgiram, ainda, ao abrigo do regime legal anterior e não ao abrigo do RGPD, já que se reportam a factos praticados antes da aplicação do diploma comunitário. Já no mais recente Relatório de Atividades de 2019/2020[262], a CNPD sancionou um total de 49 coimas, sem especificar se algumas das infrações se deviam à falta de designação e notificação de DPO à Autoridade de Controlo ou, até, à designação desadequada.

Relativamente ao desempenho das funções alistadas no artigo 39.º RGPD, deve ser interpretado como um atributo aos conhecimentos pessoais e posição que ocupa no seio organizacional. De um modo sucinto, através do artigo *supra* mencionado, fica claro que o encarregado deve prestar monitorização e aconselhamento acerca da conformidade com os normativos de proteção de dados; efetuar, direta ou indiretamente; a formação e sensibilização nestas matérias de toda a equipa organizativa, incluindo a alta direção; colaborar com as autoridades de controlo; efetuar um relacionamento constante com os

[259] Consoante análise em julho de 2021.
[260] Opinião reforçada em artigo publicado em: https://inovalegal.org/a-exigencia-multidisciplinar-do-encarregado-de-protecao-de-dados/ (consultável em julho de 2021).
[261] *In* https://www.cnpd.pt/media/fjhffphw/relatorio_201718.pdf, em 2017 foram aplicadas 160 coimas, num valor de 266 602,39 € e, no primeiro período de 2018 foram aplicadas 50 coimas num valor aproximado de 80 mil euros.
[262] *In* https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf, em 2019 das 34 coimas aplicadas pela Autoridade de Controlo, num montante de cerca de 600 mil euros, apenas 7 estão associadas a infrações ao RGPD, sendo as restantes aplicadas ao abrigo da Lei n.º67/98, de 26 de outubro, por ser o regime mais favorável a processos anteriores à aplicação do RGPD e pela Lei n.º41/2004, de 18 de agosto, sobre a privacidade nas comunicações eletrónicas. Já em 2020, ano em que os dados ficaram à mercê das alterações do quotidiano para o mundo digital, sobretudo no teletrabalho, a CNPD aplicou 15 coimas, num montante de cerca de 47 mil euros, na sua maioria relativas a infrações à legislação sobre a privacidade nas comunicações eletrónicas, sobretudo por envio de marketing direto de forma ilícita.

titulares dos dados no exercício dos seus direitos; e mais importante ainda, efetuar auditorias (periódicas ou não programadas), aconselhar em matéria de AIPD e notificar a autoridade de controlo (ou nos casos em que seja exigível, os titulares de dados) acerca da violação de dados pessoais. Às atribuições do regulamento, acrescem outras que foram redigidas na LNE conforme o artigo 11º[263]. Note-se que tais tarefas podem ser desempenhadas por um funcionário que já faça parte da empresa ou por recurso externo com base num contrato de prestação de serviços[264].

Na prática, implica que o DPO seja adequadamente envolvido em todas as questões relativas à proteção de dados pessoais (artigo 38.º nº1 do RGPD), seja capacitado dos recursos indispensáveis para o desempenho das funções e manutenção dos seus conhecimentos (artigo 38.º nº2 do RGPD), seja dotado de independência instrutória (artigo 38.º nº3 do RGPD) e autonomia técnica[265] (artigo 9.º nº2 da LNE), sem a possibilidade de vir a ser penalizado ou destituído[266] pelo exercício das suas funções (número 3 do artigo 38.º do RGPD), incumbido, ainda assim, os deveres de sigilo profissional e confidencialidade (artigo 38.º do RGPD e artigo 10.º nº1 e 2 da LNE). Só através do cumprimento integral destas nuances que circundam a figura do DPO é que ele poderá estar numa posição adequada para promover a cultura de proteção de dados na organização e, sobretudo, para dar cumprimento aos elementos essenciais do Regulamento. Na eventualidade do responsável pelo tratamento ou do subcontratado incumprirem as obrigações previstas no artigo 38.º do RGPD, tal constituirá em violações sujeitas a coima, nos termos da alínea a) do nº4 do artigo 83.º do RGPD.

Importa ressalvar que no caso da organização vir a ser sancionada pela autoridade de controlo, por se encontrar em incumprimento com a legislação comunitário ou nacional, ainda que contenha um encarregado de proteção de dados e seja cumpridora das nuances exigidas pela sua existência, a Responsabilidade pelo incumprimento será unicamente imputada ao Responsável pelo tratamento e/ou ao Subcontratado, ficando o DPO despido de Responsabilização perante a Autoridade de Controlo.

[263] Embora tal redação pareça, de certa forma, redundante e desnecessária, já que a realização de auditorias e programas de sensibilização já se encontram redigidos, ainda que em abstrato, na alínea b) *in fine* do número 1 do artigo 39.º do RGPD.
[264] *Cfr.* ANA FAZENDEIRO, *Regulamento Geral sobre a Proteção de dados*, Almedina, 3ª edição, 2018 *pág.* 20.
[265] Pode, inclusive, exercer outras funções, desde que não resultem num conflito de interesses baseados no papel que deve desempenhar – artigo 38.º nº 6 do RGPD e artigo 12.º nº5 da LNE.
[266] Tal atribuição poderá gerar interpretações contrárias ao espírito legal nos normativos laborais.

Ainda mais, qualquer responsabilidade civil ou contraordenacional que ocorra derivada de violações das disposições legais, será da incumbência do responsável pelo tratamento ou do subcontratado[267]. Mas a sua existência será fator expetável de atenuar estas mesmas consequências, sendo o ilustrador de quais caminhos percorrer para serem criadas todas as condições de salvaguarde de direitos dos titulares. Caso venha a cair no incumprimento, é presunção irrefutável de que o Responsável pelo tratamento, como o próprio nome indica, não foi capaz de transmitir os recursos necessários para o desempenho das funções do artigo 39.º ou tenha falhado na designação do Encarregado de Proteção de Dados.

Por mais claro que esteja definido, nos termos do Regulamento Geral sobre a Proteção de Dados, de que o DPO não é o responsável pela proteção de dados, o recente caso da Câmara Municipal de Lisboa em que sugiram transferências de dados pessoais, para a embaixada da Rússia, relativos aos ativistas que promoveram em janeiro uma manifestação política, suscitou a desinformação veiculada pela larga maioria da comunicação social, acerca da posição e das funções do Encarregado de Proteção de Dados[268]. Um dos motivos que se aponta para esse desalinhamento será, como referido, inicialmente, no ponto 4 do presente Capítulo, a infeliz tradução para a língua portuguesa que faz aludir o termo "encarregado" ao grau de responsabilidade sobre a matéria.

Tal desvirtuamento concetual conduziu, inclusive, a misturar as funções do DPO da autarquia, ao ponto do Presidente da Câmara Municipal de Lisboa dar a indicação de proposta ao executivo municipal acerca da "exoneração do Encarregado de Proteção de Dados e coordenação da Unidade de Projeto para a Implementação do Regulamento para a Proteção de Dados" (sublinhe-se a própria indicação incorreta do Regulamento "sobre" e não "para" a Proteção de Dados). O certo é que, tal exoneração dificilmente encontrará legitimidade para que se prossiga. Como exposto, ao EPD incumbe as funções de informação, aconselhamento, sensibilização e auditoria, exercidas de forma independente, enquanto que ao Responsável pelo tratamento (neste caso, a Câmara Municipal de Lisboa), dependerá a implementação de medidas de proteção de dados que considere conveniente. Assim sendo, o poder decisório a responsabilizar não sairá da esfera jurídica do DPO, mas sim as meras recomendações que sustentam a decisão proferida pelo Responsável pelo tratamento. Aparentemente, poderá se

[267] *Cfr.* GT29, *Guidelines on Data Protection Officers ("DPOs")*, pág. 4.
[268] Como exemplo, o artigo publicado no Diário de Notícias em que se confunde o DPO com o respetivo "responsável pela proteção de dados na autarquia", *in* https://www.dn.pt/politica/medina-assumimos-as-responsabilidades-13849775.html.

suscitar a devida penalização caso não tenha havido as devidas recomendações sobre o assunto.

No caso em apreço, a Associação dos Profissionais de Proteção e de Segurança de Dados (APDPO), em comunicado, veio repudiar a desinformação veiculada pela comunicação social e, por outro lado, defender o Encarregado de Proteção de Dados da Câmara Municipal de Lisboa, manifestando a intenção de apresentar queixa à CNPD se caso a exoneração do respetivo DPO se vier a materializar[269].

Mas qual será a extensibilidade da **responsabilidade civil profissional do DPO**? A responsabilidade pelo incumprimento do disposto no RGPD e demais legislação *data* protecionista, embora inerente a quem tenha o poder decisório – nos termos dos artigos 24.º e 30.º do RGPD – não faz com que o DPO esteja isento que qualquer responsabilidade. "À semelhança de um advogado, médico, engenheiro ou outro profissional que é contratado em virtude dos seus conhecimentos técnicos, da sua experiência, do seu *know-how*, o EPD que não cumpra, por negligência, falta de zelo ou de interesse pelas suas funções, as tarefas para as quais foi contratado/designado poderá ser profissionalmente responsabilizado pelos danos decorrentes da sua inação ou inadequada tomada de decisões"[270]. Desta forma, a averiguação do incumprimento das devidas funções dependerá da capacidade de comprovar, neste caso, advinda do próprio Encarregado de Proteção de Dados. Só através de um registo/ arquivo prudente das sugestões, recomendações e demais atuações comunicadas à administração da entidade é que o DPO poderá comprovar que a não adoção de uma decisão se deveu a inação ou à não ponderação do parecer que tenha transmitido. Sem registo da sua atividade, poderá ser também responsabilizado por não cumprimento das suas funções, o que infringe o artigo 39.º do RGPD.

4.2.2. **Prerrogativas e Atribuições**

Através da norma comunitária, são estabelecidas diversas Prerrogativas e atribuições inerentes à dignidade da figura em análise. No fundo, o exercício das suas funções na

[269] *Cfr.* https://www.dpo-portugal.pt/noticias/185-tribunal-de-justica-da-uniao-europeia-reforca-poderes-das-autoridades-nacionais-de-protecao-de-dados-2.
[270] *Cfr.* SIMÃO DE SANT'ANA e VITORINO GOUVEIA, *in* "O RGPD e os Recursos Humanos – Guia Prático para a Conformidade", Almedina, 2021, pág. 90.

organização assegura ao Encarregado de Proteção de Dados um conjunto de direitos que estão intrinsecamente associados à posição laboral privilegiada. Já enunciamos a impossibilidade de ser destituído ou penalizado e a atuação sem sofrer instruções por parte da alta direção organizativa, plasmadas no artigo 38.º nº3. Do mesmo numerado, retira-se o acesso direto à direção de alto nível da organização, o que implica uma relação obrigatoriamente direta entre o responsável e o DPO, sem intermediários para colocar questões ou propostas necessárias. O Regulamento aproveita para sublinhar que, embora a direção não possa instruir nas funções do EPD, o contacto direto não colocará essa vantagem em causa, mas antes permitirá clarificar o aconselhamento do Encarregado, pois só através do contacto entre ambos é que se poderá expressar sem alterações ou interferências das clarificações confidenciais. Tal não implica que todo o Gabinete do Encarregado de Proteção de Dados, quando exista, possa entrar em contacto diretamente com a direção, sendo uma vantagem exclusiva.

Acrescem ainda as vantagens de ser envolvido em todas as questões[271] respeitantes à temática da proteção de dados na organização e, segundo o Regulamento, esse envolvimento deve seguir de forma adequada e em tempo útil[272], isto é, com o direito de ter disponível o tempo suficiente para cumprir com suas as tarefas. O Responsável pelo tratamento ou o Subcontratado ficam com a obrigação de facultar o apoio suficiente para que o DPO exerça as suas funções – artigo 38.º nº2 do RGPD – nomeadamente, recursos financeiros, humanos e materiais, além da manutenção dos seus conhecimentos (referidos em nota de rodapé nº 85). O legislador comunitário reconhece o ponto evolutivo que o âmbito de proteção de dados atinge e que, por isso, quem esteja encarregue de aconselhar procedimentos preenchidos pelos Princípios do RGPD, deve estar minimamente atualizado quanto às alterações e à adaptação dos normativos *data* protecionistas nos diversos setores.

Por outro lado, como nenhuma figura da relação jurídica deve viver apenas de direitos, ao DPO acrescem encargos e obrigações no desempenho da sua atividade. No desenvolver dos argumentos relativos ao seu posicionamento, foram já especificadas as obrigações de sigilo e confidencialidade, a não permissão de exercer outras funções que possam gerar conflitos de interesse com as suas funções de Encarregado e o dever de conhecimentos profundos e

[271] Na prática, é sinónimo de ter acesso às operações de tratamento e a todos os dados pessoais, sempre com o dever de sigilo e confidencialidade entranhados na sua atuação interna e externa à organização.
[272] Artigo 38.º nº1 do RGPD.

especializados[273] no domínio jurídico e de boas práticas (padronizações) em matéria de proteção de dados pessoais. Dos encargos já analisados, podemos acrescentar obrigações de estar capacitado para desempenhar funções tecnológicas, e mais ainda, de ter conhecimento sobre tecnologias de informação e de segurança dos dados, estar capacitado para a promoção da cultura *data* protecionista através da promoção de ações de sensibilização interna sobre a temática e estar a par das operações de tratamento realizadas e perspetivadas pela organização. Ou seja, não é apenas um direito de poder conhecer e aceder aos dados pessoais, é sua obrigação[274].

Separadamente, outra obrigação tem por base o encargo de responder ao contacto dos titulares de dados pessoais sobre questões relacionadas com o tratamento dos dados pessoais e com o exercício dos direitos que lhes assistem - artigo 38.º nº4 do RGPD. Esta atribuição só é possível devido ao artigo 37.º nº7 do RGPD, do qual se retira a exigência imputada ao Responsável ou subcontratado em comunicar os contactos do EPD às autoridades de controlo competentes e de publicar os contactos do EPD[275].

O GT 29 na orientação "243 ver.01" adotada em 13 de dezembro de 2016 (mais concretamente no ponto 2.6), entende que este artigo assegura que o Encarregado possa vir a ser direta e facilmente contactado sem que seja necessário contactar diretamente a organização. Parece-nos que a conclusão retirada pela GT 29 em ser possível contacto por mero formulário a ser entregue diretamente no edifício da entidade ou por via eletrónica não garantiria a confidencialidade e colocaria em causa a posição de funcionários da própria entidade que quisessem apresentar queixas sobre os procedimentos desenvolvidos na organização que faça parte. Assim, os contactos do EPD devem incluir *"informações que permitam aos titulares dos dados e às autoridades de controlo contactar facilmente o EPD (endereço postal, número de telefone e/ou endereço de correio eletrónico)"*. Fica em dúvida a questão sobre o meio pelo qual esses contactos devem ser publicados.

[273] Dever abstrato com pouca probabilidade de ser passível de comprovação, pelo menos nos primeiros anos de pós RGPD. Um encarregado poderá ser entendido como suficientemente especializado para desempenhar as funções, na medida do que seja o contexto da entidade que exerça as funções. O próprio legislador nacional não exige qualquer certificação profissional para que esteja em posição de elegibilidade, reforce-se.

[274] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 100.

[275] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 98.

Escassas são as vezes em que os contactos do Responsável pelo Tratamento vêm acompanhados dos contactos do Encarregado de proteção de dados, aquando do preenchimento do formulário sobre o consentir o tratamento de dados pessoais. Algumas entidades privadas optam por incluir os contactos do EPD na vasta e exaustiva política de privacidade, mas não são poucas as entidades que ainda não têm essa publicitação no documento. Nestes casos fica a dúvida: o titular dos dados pessoais, por exemplo, um funcionário que não quer que a entidade patronal saiba acerca da sua contestação, quererá entrar em contacto direto com o DPO, mas após uma longa procura não encontra esses contactos. Quando o regulamento exige esta publicitação, está ciente que tal publicitação (entenda-se pública, logicamente) deve seguir vias intuitivas para um cidadão comum. Caso contrário, parece-nos estar já em posição desconforme com o disposto no Regulamento. O certo é que, também não surgiram, para já, qualquer aplicação de coimas (segundo a base de dados que temos vindo a acompanhar) ou, pelos vistos, qualquer intervenção pedagógica para vir a alterar os meios de publicitação, de modo a clarificar os pontos de contacto direto.

CAPÍTULO III – Implementação Prática do RGPD, o Papel do EPD

Em todas as disposições normativas, a concretização prática só poderá ser alcançada se a redação tiver capacidade para transmitir as concretas implicações que dela se estabeleçam, de forma clara e precisa, nos seus destinatários. No caso do RGPD, os destinatários serão aqueles que se vêm encarregues de estar em conformidade, mas, sobretudo, todos os que se encontram na qualidade de titulares de dados.

Após a compilação bibliográfica[276] acerca dos caminhos a percorrer para que as entidades garantam a sua *compliance* com o Regulamento, descomplicando o regime jurídico em fases de concretização, conclui-se que existem dois momentos cruciais a serem distinguidos: o primeiro passa pela adequação inicial com os encargos retirados do RGPD, isto é, o primeiro contacto para efetuar as alterações de conformidade. É um momento que, pela generalidade já ter ultrapassado, será estipulado por análise prática, sucinta; o segundo, é o momento em que se encontram a larga maioria das entidades, de pós adequação e constante atualização e monitorização do estado de conformidade. É o momento constante e comprovado de que estar em conformidade com a proteção de dados pessoais é um processo constante.

No seguimento de um conjunto de noções, orientações e reflexões decorrentes do disposto no RGPD, e estando já enquadrada a pegada do Encarregado de Proteção de dados na relação jurídica *data* protecionista, passamos a uma análise prática diretamente vocacionada sobre a implementação do Regulamento e o papel fulcral do DPO (e demais equipa colaboradora) para manter o vínculo à conformidade.

[276] Recorremos ao curso breve de "RGPD para implementadores na Administração Pública" disponibilizado na plataforma da "NAU – Sempre a Aprender", em parceria com a "INA – Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas", consultável em www.nau.edu.pt/curso/rgpd-para-implementadores-na-administracao-publica/ (disponível em Dezembro de 2020); Foram, igualmente, consultados os livros "RGPD Guia para uma auditoria de conformidade" da FCA – Editora de Informática, Lda., pelo autor Nuno Saldanha e "Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria" da EDIÇÕES ALMEDINA, S.A., pelos autores Daniel Alves da Cunha, Ana Hierro e Diogo Rodrigues da Silva.

1. Processo de Adequação Inicial

De modo a que a entidade se adeque às exigências decorrentes da norma comunitária, primeiro que tudo é determinante clarificar a matriz das responsabilidades, isto é, quem desempenha a figura de Responsável pelo tratamento (pela implementação[277]), quem ficará como elemento chave em cada setor/unidade orgânica para cooperação simultânea e, se nesta fase já for possível, quem é a figura encarregue pela *compliance* (DPO). Afigura-se uma vantagem primordial se o Encarregado de Proteção de Dados for corretamente designado no primeiro passo à implementação das medidas, ficando intimamente capaz de conhecer o contexto organizacional que determinará a sua atuação no momento de pós adequação. Mas a sua ausência até as fases finais da implementação não a colocará em causa.

Algumas entidades até entendem que ficam numa posição mais justa de designar o EPD correto, após a exaustiva análise da caraterização e orçamentação internas. Caberá, portanto, ao entendimento de cada organização em nomear no primeiro passo ou na conclusão do "desenho" de adequação. O certo é que, todo o processo será iniciado na primeira reunião de trabalho composta pelo Responsável pelo tratamento (possivelmente, pelos seus subcontratados que já existam), pelos auditores de dados[278] e pelos representantes dos setores jurídicos, de recursos humanos e de sistemas de informação, com o objetivo de caraterização geral dos fluxos de dados da entidade[279].

A partir do primeiro contacto de adequação a entidade terá que fazer jus ao Princípio da Responsabilidade, da capacidade de demonstrar a conformidade, através de um registo rigoroso das suas atuações seja por via de formulários ou de atas assinadas pelos presentes. Da primeira reunião é alcançada a concreta dimensão dos trabalhos necessários e a orçamentação aproximada que acarretem[280].

Vejamos um guia meramente exemplificativo das fases percorridas após planear o projeto de conformidade, para ser concluída a adequação inicial:

[277] O dirigente máximo da organização.
[278] Auditores internos ou em regime de *outsourcing*.
[279] Já nesta reunião a entidade retira a vantagem de conhecer melhor os seus processos de gestão de informação, isto é, os seus sistemas utilizados (de base automatizada, computacional, manual ou até humana) não só de conotação pessoal, mas também concorrencial.
[280] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs.15 e 16.

a) Diagnóstico Interno e Mapeamento de Dados

Composto por um "diagrama de fluxo de dados" que ilustra o volume e diversidade de dados tratados pela entidade consoante uma perceção clara, reunindo as operações de tratamento, as categorias de dados, os titulares que estejam afetos, as entidades subcontratadas e outras nuances de um diagnóstico empírico capaz de percecionar quais os ajustamentos gerais a tomar em linha de conta. Efetua-se uma análise ao arquivo, à organização interna e a disposição dos postos de trabalho, sendo necessárias visitas às diversas instalações que pertençam ao organismo, alcançando uma representação macro dos processos de dados[281]. Ninguém descomplicará melhor o processo do que aquele que realize esse mesmo tratamento, pois só os colaboradores de cada "terreno" é que clarificam as "rotinas" criadas na prática diária (combate a uma visão macro, externa à real vivência da entidade).

A inventariação deve ser exaustiva e, para tal, deve ser efetuado o levantamento por cada setor ou unidade orgânica acerca dos dados pessoais, dos intervenientes que os processam e das formas como são processados. Na prática a inventariação será realizável através de um formulário de recolha e classificação dos materiais onde haja a presença de dados pessoais (contratos, questionários, documentos de logística, etc.) e depois, um formulário de classificação dos dados pessoais, além da verificação da licitude no seu tratamento. Assim, a entidade será portadora de uma compilação detalhada de ações de conformidade necessárias[282]. Poderá ser relevante a restruturação dos processos no modelo de Macroestrutura Funcional (MEF) utilizado para melhorar a eficácia da gestão documental e assim, auxiliar no levantamento do processos negociais.

b) Avaliação de Conformidades e Implementação de Correções

Com a inventariação das medidas de segurança já existentes e dos riscos internos e externos associados, nesta fase importa verificar as bases legais associadas ao tratamento de cada dado, às políticas, regulamentos, procedimentos[283] e processos de gestão de dados

[281] Será distinto consoante a dimensão e modelo contextual da entidade. Se estiver em causa uma fábrica de papel composta por 200 trabalhadores a intervenção e adequação estará mais direcionada para os recursos humanos, enquanto que uma empresa de *software* composta por 50 trabalhadores verá a sua intervenção mais direcionada para os sistemas de gestão de informação.

[282] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 20 a 29.

[283] Caso não existam, consoante os *standards* internacionalmente recomendados, é nesta fase que são desenvolvidas e aperfeiçoadas as medidas de segurança organizacionais em geral (essencialmente a Política de Privacidade da organização, políticas de acesso e permissão ao tratamento – onde é recomendável a dupla autenticação - medidas de gestão e prevenção de risco e a avaliação do nível de segurança

instaurados no seio organizacional. Poderá ser desenvolvida no decurso da fase anterior, mas em separado permitirá um arquivo documental mais exaustivo. Nesta fase, a equipa de implementação deve ser portadora de conhecimentos profundos dos princípios oriundo do RGPD e dos direitos dos titulares de dados pessoais. Só assim é que é possível desenhar correção permanentes e não meras alterações pontuais. Das implementações mais significantes nesta fase, será o plano de tratamento do risco de segurança da informação (ter ciente a ideia do risco iminente). Atinge-se os primeiros passos da implementação em concreto[284].

c) Aperfeiçoamento dos Procedimentos e Processos

Fase pela qual a equipa intervém nos processos relativos à relação com o titular dos dados e com a autoridade de controlo[285], por forma a cumprir com direitos dos titulares e com o Princípios do Regulamento, por exemplo, os processos que garantem o direito de retificação ou atualização, o direito de informação, o direito de esquecimento, entre outros. A equipa de implementação deve direcionar as melhorias necessárias para cumprir com a conformidade e priorizar os designados "*quick* wins" – aperfeiçoamentos céleres e de baixo investimento. A forma como a atividade organizacional é realizada, manual ou informatizada, não poderá interferir com os preceitos da legislação internacional, comunitária e nacional da proteção de dados pessoais. Na prática, a organização tem ao seu dispor um mercado de ferramentas informáticas eficientes para desenhar os processos. Os processos serão aperfeiçoados[286] consoante um espírito interfuncional, sistemática e não tendo em conta os setores ou unidade orgânica separados entre si. Só assim a correção, por exemplo, de um erro num dado pessoal pedida pelo seu titular irá desaparecer em todos o sistema, feita de uma só fez, sem redundância do erro.

Toda esta fase seguirá as metas já alcançadas pelas fases anteriores, nomeadamente, com o inventário de medidas de segurança em falta, em que se retificam desconformidades que são prioritárias e que colocam um nível de risco mais elevado, consoante a caraterização dos

alcançável nos sistemas e aplicativos informáticos, etc). Importará, igualmente, o reforço nas medidas de segurança física que podem parecer desconexas com o Regulamento, mas a sua revisão permite garantir a Segurança plena da Privacidade dos dados.

[284] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 30 a 34.

[285] Essencialmente na notificação dos casos de violação de dados pessoais.

[286] Preenchem as regras de simplificação, intuição, interoperabilidade, de acesso e linguagem simples, entendível internacionalmente – normas BPMN (*Business Process Management Notation*).

dados pessoais da organização, podendo agilizar onde terá maior necessidade em atuar e corrigir de forma mais imediata[287].

Será o ponto de implementação ao qual as campanhas de sensibilização internas serão fundamentais para garantir uma boa comunicação entre a equipa de implementadores e todos os colaboradores da entidade. Através da sensibilização é possível passar a mensagem que não se trata de uma implicância para com um funcionário, mas sim todo um processo novo que a entidade tem de estar mentalizada, exigindo alguma compreensão e humildade por parte de todos os intervenientes para que as correções tenham os efeitos pretendidos.

d) Implementação de Medidas de Compatibilidade Tecnológica

Fase de projeção e apelo à adequada intervenção técnica de equipas especializadas nos sistemas de informação, consoante a orçamentação estipulada pela alta direção. Há o levantamento de aspetos relativos às medidas técnicas mais adequadas para garantir a segurança recomendável do tratamento, tendo em conta a tecnologia disponível, além do respeito pelo princípio da proteção de dados pessoais desde a conceção e por defeito, a criação de mecanismos adequados para futura comunicação de violação de dados pessoais aos titulares dos dados e para o cumprimento de futuros pedidos circundantes ao direito ao apagamento, à atualização ou à portabilidade dos dados[288].

As entidades privadas poderão ser beneficiarias de uma posição clarividente de conformidade nesta fase se efetuarem o cumprimento das recomendações sobre requisitos técnicos mínimos das redes e sistemas de informação exigidos às entidades públicas consoante a Resolução do Conselho de Ministros nº41/2018, de 28 de março. São, portanto, linhas orientadoras impostas às entidades públicas, mas que auxiliam na tarefa de adequar os termos tecnológicos para o cumprimento do Regulamento também para os auditores que executem funções para as tais entidades privadas. As normas ISO 27002 terão, também, o papel predominante nesta matéria.

[287] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 36 a 40.
[288] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, págs. 41 a 45.

e) Elaboração de Dossiê de Auditorias

Esta fase é o culminar de todo o resultado alcançável e perspetivado. Trata-se do reconhecimento de que o papel de uma entidade em *compliance* não fica pela mera implementação. Parte, de seguida, para uma auditoria de conformidade capaz de rever e avaliar a adequação dos processos de tratamento de dados pessoais. Num processo de auditoria "São muitas as questões a analisar neste tipo de trabalhos que não se ficam apenas pela simples análise da forma como os dados pessoais são geridos. Falamos da necessidade de verificação da equipa de proteção de dados, da análise que é feita, ou deverá ser feita (…) e, claro está, do *reporting* (reporte, em português), porque sem análise do que se faz, e do conhecimento e registo dos trabalhos efetuados, será sempre mais difícil analisar o passado e perspetivar o futuro" (*Ob. Cit.* Nuno Saldanha, 2018)[289]. Além disso, deixa projetada a forma como futuras auditorias devem ser prosseguidas: em intervalos planeados, por forma inesperada, com verificação de quais setores e procedimentos auditáveis e priorizáveis, por respeito aos procedimentos que se encontrem acompanhados de um nível de risco mais elevado). É a forma incontornável de comprovar o esforço de conformidade e de adequação contínua – preenche as evidências exigidas no artigo 24.º nº1 do RGPD.

Do dossiê de auditoria de conformidade deve constar o registo das atividades de tratamento totalmente atualizado linearmente. É um mecanismo que tem início na implementação, mas que continuará obrigatoriamente na fase de pós adequação, pois por cada vez que se alterar o tratamento, este terá que ser atualizado no dossiê. É nele que as funções do DPO irão se basear, contendo a descrição de todos os dados e operações de tratamento que contemplam a entidade. Por esse motivo, o dossiê ficará na posse do EPD, por meio físico ou digital, figura que será essencial para verificar se a organização continua a funcionar em conformidade[290].

[289] Cfr. NUNO SALDANHA, *RGPD guia para uma auditoria de conformidade – Dados, Privacidade, Implementação, Controlo, Compliance*, FCA, 2018, *Ob. Cit.* Pág. XV.
[290] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 78.

f) Formação dos Colaboradores e Verificação dos Aspetos Implementados

É a etapa conclusiva da implementação do Regulamento, focada nos resultados do que tenha vindo a ser projetado. Verifica-se a eficiência dos procedimentos sujeitos a alterações e a interiorização do novo enquadramento da proteção de dados pessoais, na forma de trabalhar dos colaboradores. Será realizada a formação e consciencialização para o exercício das tarefas individuais de cada trabalhador, em conformidade com os normativos *data* protecionistas. A promoção da cultura de proteção de dados no contexto interno da entidade permite que, mais do que implementada, seja praticada diariamente a conformidade de forma consciente, sistemática e plena de ética profissional[291]. É a entrada para o processo contínuo de adequação.

2. O papel do EPD após a Implementação do RGPD na Organização

Com a implementação efetuada, ao Encarregado de Proteção de Dados passará a caber especial "responsabilidade" em continuar a informar e aconselhar sobre alterações legislativas, pareceres e deliberações da CNPD, tanto ao Responsável pelo tratamento ou ao subcontratado, quanto aos funcionários da entidade em causa. Por este facto é que seria relevante o DPO integrar na equipa de auditores de implementação desde a primeira etapa, por forma a dar continuidade à intervenção tendo por base o reconhecimento do contexto e orçamentação disponível da entidade. Não implicará apenas a informação acerca das alterações legislativas, mas também atualização das práticas recomendáveis, consoante as evoluções tecnológicas e o âmbito negocial que esteja patente. É um elemento que deve ser, portanto, designado pela sua real versatilidade e criatividade no desenvolvimento da atividade, relevando tanto as suas capacidades pessoais, como o nível de ética profissional e de compromisso com a tarefa primordial que fica encarregue.

Das funções pelas quais esteja vinculado a efetuar, passaremos a ilustrar conclusivamente:

[291] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 100.

2.1. Auditorias de Conformidade

Tendo por base a *compliance* contínua requisitada nos artigos 5.º nº2 e 24.º do RGPD, caberá ao EPD fiscalizar sucessivamente se as atividades desenvolvidas preenchem o cumprimento da situação de legalidade. Além de realização de formações ou *workshops*[292], a fiscalização passará pela realização de auditorias de forma regular, com a sua periocidade a variar[293] consoante os fatores de risco existente, a dimensão estrutural da entidade, escala de titulares e de dados pessoais sensíveis, o tipo de operações de tratamento executadas, mas também o valor empregue na contratação do DPO[294].

As auditorias de conformidade pressupõem a visita e inspeção às instalações e mecanismos onde são processados dados pessoais, após efetuar uma reunião presencial entre os auditores e o DPO na qual se projete qual o levantamento da informação que deve ser vistoriada. Tem a finalidade de avaliar a atuação da entidade, verificar a implementação efetiva de novas indicações e ponderar sobre a necessidade de novas recomendações[295]. As medidas alternativas de implementação devem estar enquadradas na legislação vigente e não podem infringir no normal funcionamento do negócio ou atividade desenvolvida, o que exige uma sensibilização ponderada com capacidade de entender os efeitos práticos decorrentes da sua aplicabilidade[296]. Caso prejudiquem esse normal funcionamento da atividade, terão maior probabilidade a reprovação do Responsável pelo tratamento, ficando a desconformidade detetada por resolver.

A auditoria de conformidade transversal será documentada detalhadamente[297] em relatório para que se salvaguarde a prova de conformidade perante uma eventual fiscalização da CNPD ou por efeitos de denúncia ou reclamação dos titulares de dados e deve ter caráter

[292] Quando se afigure necessário um reforço dos conhecimentos na generalidade da organização.
[293] São aconselháveis três auditorias por ano, dependendo dos fatores em causa, mas em nenhuma situação poderá ser passível de comprovação de conformidade sem, pelo menos, ter documentada uma auditoria anual.
[294] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 104.
[295] Além de novas recomendações, poderá ser necessário a atualização de medidas outrora recomendadas. Exemplo claro são as limitações de acesso que tendem a ser atualizadas, pelo menos uma vez por ano, fruto de eventuais alterações procedimentais internas, como a mudança de funções a desempenhar por colaborador que já fazia parte da entidade ou pela contratação e despedimentos que possam ocorrer. Acrescem ainda alterações na estrutura das instalações que, sem a devida atualização das medidas físicas, poderão suscitar o agravamento do risco e a desconformidade.
[296] É nesta vertente que auditores com especialização em gestão e/ou recursos humanos são fundamentais.
[297] Transpareça que tenham sido analisados os diversos aspetos de tratamento de dados pessoais (clientes, utilizadores da via eletrónica, bases de dados de funcionários e colaboradores), as medidas de informação, comunicação e transparência, as medidas de segurança e privacidade implementadas desde a autoria anterior e quais as recomendadas para implementação futura. No domínio jurídico, devem documentar o número de AIPD e de consultas prévias que tenham sido, desde então, realizadas, os pedidos de exercício de direitos por parte dos titulares de dados e o nível de eficácia da resposta, como também o número de violações de dados ocorridas.

confidencial, tendo um número restrito de elementos internos com possibilidade de consulta do referido relatório.

2.2. Promoção de Testes Vulnerabilidades

A equipa multifacetada de auditores de dados, conjuntamente com os pareceres manifestados pelo DPO, podem executar testes regulares de "intrusão" (na denominação inglês *pentesting*). São mecanismos relevantes para averiguar a eficiência das medidas (novas ou implementadas desde a auditoria inicial) e documentar a eventual vulnerabilidade e riscos que ainda possam existir[298]. Claro está, o risco ainda que seja insignificante ao ponto de ser passível de vivência com a atividade desenvolvida, ele terá de ser reconhecido e documentado – artigo 32.º nº2 do RGPD.

Os auditores de dados que cooperem com o EPD, poderão fundamentar o âmbito da testagem de penetração[299]. Tendencialmente, são executados testes regulares de recuperação aos *backups*, às *firewalls* e antivírus, aos mecanismos de DLP, entre outros, por forma a averiguar a resiliência dos sistemas tecnológicos, verificando a sua capacidade para impedir a ocorrência de violações de dados e de recuperação dos mesmos em caso de perda. Estas medidas deverão ser registadas em relatórios (individualmente ou no corpo do relatório de auditoria de conformidade).

2.3. O Parecer nas Avaliações de Impacto da Proteção de Dados[300]

Quando as operações de tratamento de dados pessoais suscitarem dúvidas sobre a sua implicância na elevação do risco para os direitos e liberdades das pessoas singulares, antes de ser efetuado esse tratamento deverá ser realizada uma AIPD[301] "*a fim de avaliar a*

[298] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 107.

[299] Fazem o papel de *hackers maliciosos* e verificam as vulnerabilidades existentes no sistema de atividade. É conveniente que o testador que penetre o sistema tenha formação em ataques éticos, já que ao encontrar o sistema vulnerável, terá em sua mão informações confidenciais, capazes de abater a entidade. Se o Responsável pelo tratamento ou subcontratado optar por designar, por via de prestação de serviços informáticos, uma entidade externa para efetuar estas medidas de avaliação, terá de garantir que toda a atuação seja executada sob a autoridade da entidade responsável, seguindo exclusivamente as suas instruções (artigo 32.º nº4 do RGPD) – o que não ocorre se forem efetuadas pelo próprio EPD, livre de instruções.

[300] *Cfr.* FERNANDA MAÇÃS e FILIPA CALVÃO *in O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas – notas breves para a compreensão do seu estatuto,* Fórum de Proteção de dados (CNPD), n.º 07, dezembro de 2020, pág. 54.

[301] Na sua terminologia inglesa é um processo reconhecido como DPIA – *Data Protection Impact Assessment*

probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco" – Considerando nº 90 do RGPD.

Trata-se de um processo contínuo e dinâmico de avaliação destinado a estabelecer e comprovar a conformidade do tratamento de dados pessoais, sendo que na sua análise será avaliado o tratamento, na medida dos critérios de necessidade e proporcionalidade, e concluirá sobre os riscos que possam advir desse tratamento para os direitos e liberdades das pessoas singulares, isto é que consequências recai na esfera jurídica do titular dos dados. É o método essencial para gerir os riscos regularmente, efetuar a devida identificação, análise, avaliação e atenuação que recai sob o Responsável pelo tratamento, segundo as orientações do GT 29[302]. São inclusive partilhadas metodologias e formas de documentar a AIPD nos *guidelines* do GT 29.

Mas nem todos as operações de tratamento estão obrigatoriamente sujeitas à realização de uma AIPD. O Regulamento estabelece o dever das Autoridades de controlo[303] elaborarem e publicitarem uma listagem taxativa dos tipos de tratamentos que sejam obrigatoriamente sujeitos a Avaliação do Impacto, antes da sua execução. Por outro lado, deixa a critério de cada Autoridade de Controlo a publicação de uma outra listagem que clarifique as operações de tratamento em que não seja, de todo, necessária a execução de uma AIPD[304]. A CNPD cumpriu o dever de listar as operações de tratamento sujeitas a AIPD por via do Regulamento nº1/2018, enquanto imposição de natureza normativa[305], geral e abstrata sobre o dever de realizar a AIPD, podendo ser alterada consoante a evolução científica e tecnológica que vier a se revelar significante neste âmbito. Excecionalmente, se um conjunto de operações de tratamento incidirem sobre risco semelhante, poderão estar sujeitas a uma única avaliação. Nas situações em que não haja essa obrigação, o Responsável poderá implementar,

[302] WP 248 rev.01 e WP 251 rev.01 – implica uma descrição sistemática e transparente das operações de tratamento e finalidade subjacentes, avaliadas por critérios de proporcionalidade e necessidade; uma avaliação e gestão adequada dos riscos de infringir os direitos e liberdades das pessoas singulares; identificação de medidas de mitigação de riscos que se afigurem necessárias, com auxílio da certificação conferida pela norma ISO 31000/2018. Alguns aspetos formais devem ainda fazer parte da AIPD, nomeadamente, a designação direta e inequívoca dos tratamentos alvo de avaliação, determinação da periodicidade a que foi realização tal avaliação, a verificação de consulta prévia obrigatória à CNPD e a documentação integral de todo o processo de avaliação em análise.

[303] Consagrado no artigo 35.º nº4 do RGPD e reforçado na LNE pelo seu artigo 6.º nº1, alínea c). A própria norma nacional de execução estabelece que tal publicação deve ser feita via *website* – artigo 7º nº3 da LNE.

[304] Artigo 35.º nº5 do RGPD, referenciado no artigo 7.º nº1 da LNE.

[305] A não concretização eficaz da AIPD (seja por não realização ou por realização de forma incorreta) implicará uma contraordenação suscetível de aplicar uma coima até 10.000.000,00 euros ou até 2% do volume empresarial de negócios anual, correspondente ao exercício financeiro anterior – artigo 38.º nº1, alínea l) da LNE e artigo 83.º nº4, alínea a) do RGPD)

facultativamente, uma avaliação de impacto desde que fundada no bom cumprimento do seu dever de proteção de dados pessoais.

Do número 9 do artigo 35.º do RGPD retira-se um facto curioso: o Responsável pelo tratamento deve solicitar a opinião dos titulares de dados pessoais, sempre que necessário desde que não afete os interesses comerciais ou da segurança do tratamento. Parece-nos invulgar que tal ocorra na prática. É mais frequente o Responsável solicitar um parecer da CNPD sempre que necessário, por via de consulta prévia – artigo 36.º nº1 do RGPD.

Já o encarregado de proteção de dados, embora não possa realizar diretamente a avaliação de impacto[306], posto que está vinculado a uma função de fiscalização sem conflituar interesses, este tem o dever de emitir um parecer relativo à AIPD em resposta à solicitação que recai sobre o Responsável pelo tratamento no artigo 35.º nº2 do RGPD. Ademais, a figura do EPD dará o seu contributo como ponto de contacto com a autoridade de controlo[307] quando o Responsável pelo tratamento tiver a obrigação de consultar previamente a CNPD[308], segundo o artigo 36.º do RGPD, no sentido de averiguar se é possível a realização das operações de tratamento sujeitas à AIPD[309].

2.4. A Comunicação de Violações de Dados Pessoais[310]

O regulamento reconhece que o amplo terreno onde pode ser efetuado o tratamento de dados pessoais, mesmo que cumpridor de todos os normativos e orientações de boa prática não será imune de surgir violações de dados pessoais, o que reforça também a cultura de risco nunca poder ser de nível zero. Mas, por forma a clarificar a conceituação, estabelece uma definição no ponto 12 do seu artigo 4.º sobre o que deve ser entendido como "violação de dados pessoais", conceito mais abrangente do que a expressão inglesa que tenderia a caraterizar este fenómeno — *data breach*[311]*.* Basta causar risco elevado de violar as

[306] Nada impede que faça uma análise prévia e contextualizada para auxiliar os auditores de dados. Até porque a sua fundamentação será útil para verificar as condições de licitude do tratamento e os procedimentos necessários a preencher na AIPD. Além do parecer, tem relevância na verificação da *compliance* na fase prévia e durante a realização da Avaliação de Impacto.
[307] Artigo 39.º nº1, alínea e) do RGPD.
[308] Ocorre quando se conclui pela AIPD que resultaria um elevado risco se for posto em prática o tratamento objeto de avaliação. Tal consulta será prévia à execução do tratamento, mas posterior à conclusão da AIPD, por forma a que a CNPD tenha em sua posse a casuística detalhada.
[309] ISO 29134
[310] *Cfr.* DANIEL CUNHA, ANA HIERRO e DIOGO SILVA, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria,* Almedina, 2020, pág. 114 a 116.
[311] A expressão inglesa poderá ser utilizada desde que seja interpretada consoante a definição do artigo 4º ponto 12 do RGPD.

componentes de disponibilidade, integridade e confidencialidade para que se considere violação de dados pessoais[312].

Será com base no critério de risco que determinará a obrigação de notificar a autoridade de controlo (artigo 33.º) e, em alguns casos, de comunicar essa mesma violação de dados pessoais ao titular dos dados pessoais lesados (artigo 34.º).

Nos casos da obrigação de notificação à autoridade de controlo[313], o Responsável fica obrigado a informar a autoridade de controlo competente nos termos do artigo 55.º acerca dessa ocorrência, sem demora justificada[314], se possível, no prazo de 72 horas após o conhecimento da mesma, sob pena de ser acompanhada dos motivos justificativos de atraso.

Caso seja designado um DPO, a realização da notificação poderá ser feita por este, em nome da entidade, desde que cumpra com os requisitos formais da notificação e que seja recolhida informações do incidente junto de quem se encontre apto a fornecer esses detalhes de forma inequívoca. Terá um papel imprescindível para cooperar com a Autoridade de Controlo[315] competente, sobretudo se da notificação da violação resultar uma intervenção da CNPD para solicitar esclarecimentos em relação ao ocorrido (por respeito as funções e competências da CNPD, resultantes dos artigos 57.º e 58.º do RGPD e do artigo 6.º da LNE). É aqui que pesará a existência do arquivo documental sobre a auditoria inicial, auditorias de conformidade, e realização de AIPD. No contexto nacional, esta notificação é efetuada através do preenchimento do formulário disponível no site oficial da CNPD, ou por via de outro formulário próprio, nos casos em que sejam faseadamente fornecidas as informações acerca da violação de dados pessoais – artigo 33.º nº4 do RGPD.

Por seu turno, se da violação de dados pessoais pressupor sujeição à necessidade de comunicar aos respetivos titulares dos dados pessoais, nos tramites do artigo 34.º nº1[316] (apenas quando o incidente represente "elevado risco" para os seus direitos e liberdades

[312] *Cfr.* WP 250 rev.01 (2018) – *guidelines on Personal Data Breach Notification under Regulation 2016/679*.
[313] Caso a violação seja do conhecimento do subcontratado, deverá notificar o Responsável pelo Tratamento, logo após o conhecimento desse facto, sendo unicamente ao Responsável que recai a avaliação do risco.
[314] Ter em consideração a natureza e gravidade da violação de dados pessoais em causa, além dos efeitos adversos que se retire para com o titular dos dados pessoais.
[315] Artigo 39.º nº1, alínea d) do RGPD.
[316] Obrigação de notificação ao titular dos dados pessoais, não será exigível se se verificar as condições elencadas no número 3 do artigo 34.º do RGPD, designadamente: se existirem previamente ou subsequentemente à violação, certas medidas técnicas e organizacionais suficientes para a tutela dos respetivos titulares (por exemplo, a cifragem que torna os dados incompreensíveis quando acedidos por pessoa não autorizada); caso a comunicação implique um esforço desproporcionado (por exemplo, quando exista um número elevado de titulares), situação em que deverá ser procedida uma comunicação pública generalizada, desde que garanta o mesmo nível de eficácia de informação exigida para a comunicação individual.

fundamentais), tal notificação será transmitida no momento razoavelmente possível (aferindo casuisticamente e tendo em atenção os riscos que exijam uma pronta comunicação). A sua redação deve seguir uma linguagem simples e universal, de fácil compreensão para o cidadão comum. Será composta pelo preenchimento de requisitos formais, nomeadamente, com o nome e os contactos do DPO, a descrição da natureza da violação dos dados pessoais, as recomendações atenuáveis das potenciais consequências adversas e mecanismos passiveis de execução por parte da pessoa singular em causa. Ressalve-se que poderá ser exigida a notificação aos titulares dos dados, por imposição da CNPD quando considere haver uma probabilidade de a violação resultar num elevado risco – artigo 34.º nº4 do RGPD.

De tudo isto se depreende que o responsável pelo tratamento, tal como no contexto da notificação da violação de dados pessoais a ser entrega à Autoridade de controlo competente, poderá também aqui servir-se do EPD que deverá dar o seu parecer e recomendar que seja documentada (em ata, em relatório, ou outra forma de documentação) a violação que tenha sido reconhecida, de uma forma exaustiva e complementada com o próprio formulário de notificação e, caso exista consubstanciação da prática de um crime, a cópia do auto de denúncia às autoridades de controlo.

Toda a atuação anterior dos auditores de dados, como também do Encarregado de proteção de dados, no contexto de implementação, testagem e avaliação dos procedimentos aplicáveis à notificação das violações de dados pessoais[317], serão fator determinante para cumprir com os prazos legalmente estabelecidos para as notificações e, ainda mais, mitigar, o mais rápido possível, os danos variados (físicos, materiais, imateriais). A eficácia de atuação perante uma violação de dados pessoais dependerá da existência de uma política eficaz de resposta que inclua um plano de ação rápido, recorrendo a sistemas de informação seguros. Voltamos à relevância das medidas técnicas, físicas e organizacionais.

Fica a dúvida se o EPD fique sujeito a proceder às notificações, caso o Responsável pelo tratamento opte por estar em desconformidade, nesse aspeto, em prol da imagem e credibilidade depositada na organização. Haverá um equilíbrio ponderado entre o dever de

[317] Quando projetados e implementados, devem ter em conta a existência ou não de proteção de dados pessoais por intermédio de medidas técnicas e organizacionais, mas também os legítimos interesses da entidade e das autoridades policiais, por forma a não infringir com a investigação a praticar.

sigilo e confidencialidade (artigo 38.º nº5 do RGPD) e o dever de cooperação com a Autoridade de Controlo (artigo 39.º nº 1, alínea d) do RGPD).

Considerações Finais

Concludentemente, caberá tecer considerações e perspetivas suscetíveis de evidenciar as principais ideias a reter da investigação.

Cumpre, desde logo, sublinhar que a aplicabilidade prática das exigências oriundas da atual legislação, mais rigorosa para com os Responsáveis pelo tratamento, é indiscutivelmente dependente de padrões internacionais reconhecidos como orientadores adequados à proteção da informação privada, consoante os recursos e tecnologias disponíveis de cada organização. A concretização do estado de *compliance* ficará pendente do acompanhamento de orientações internacionais, nomeadamente das Normas ISO, por forma a salvaguardar os dados na plenitude do seu ciclo vital. Será sempre evitável o surgimento de violações de dados pessoais, mas a sua existência nunca deixará de se perspetivar. A questão do próprio Regulamento comunitário vir a reconhecer essa violação, estipulando as formalidades a serem preenchidas nessas circunstâncias, é espírito idêntico ao decorrente da Gestão de Riscos (o Risco nunca poderá ser classificado por zero ou inexistente, haverá sempre a hipótese dele ocorrer e a atuação adequada das organizações é que fará com que as suas consequências inflijam mais ou menos a esfera jurídica de cada Sujeito).

Sublinhe-se, ainda assim, que as Normas ISO, no essencial, a família de normas ISO 27000, não pode ser encarada como a certificação para o RGPD, ou o *standard* para o cumprimento do Regulamento. Isto porque o objetivo do RGPD centra-se na "proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", enquanto que a ISO 27001, na sua introdução, confirma que permite o "fornecimento de requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão de Segurança de Informação" (que em conjunto com a ISO 27002 oferece controlos sobre os riscos de segurança e criar esse sistema). A segurança é fulcral para a proteção de dados, mas os moldes da ISO 27001 enquadram nos ativos de informação, para reduzir os riscos da organização, indo além dos dados pessoais, designadamente as informações confidenciais, de propriedade intelectual, *et cetera*. O RGPD refere-se à segurança nos termos dos riscos associados ao tratamento de dados pessoais e aos direitos e liberdades dos titulares desses dados (portanto, a um patamar de riscos que preenche uma dimensão dos riscos gerais de uma organização). Além do exposto, a Segurança

dos dados, ainda que imprescindível, preenche apenas um dos sete princípios do artigo 5.º do RGPD[318]. Ainda que não seja certificação direta, será de relevar que a sua estrutura é um ponto essencial para garantir a Segurança dos Dados, inclusive os pessoais. Mais ainda quando estejamos a moldar a organização à certificação da ISO 27701:2019, da qual segue uma estrutura idêntica à ISO 27001, mas voltada para a concretização de parte das obrigações emanadas pelo RGPD. A principal diferença é que a ISO 27701 pretende orientar a estrutura organizacional da entidade em prol da informação privada, enquanto que o RGPD a figura central é o titular de dados pessoais.

Ora, por uma análise estatística da certificação ISO 27001 nas empresas do EEE, a escassa relevância verificada é surpreendente. Por consideração da base de dados da Eurostat, em 2018 (ano da entrada em vigor do RGPD), verifica-se que nos 27 países da UE (já com a exclusão do Reino Unido), conjugados com os três países que configuram o EEE, existiam 25 600 000 (aprox.) empresas ativas[319], que representam a maioria dos Responsáveis pelo tratamento aos quais o Regulamento é diretamente aplicável. Segundo os dados apresentados pela Pesquisa ISO 2019[320], existem 9233 certificações válidas pela ISO/IEC 27001:2013 (número estimado) nos Estados Membros da União Europeia, na Noruega, na Islândia e no Liechtenstein. Tal se consubstancia num percentual aproximado de 0.36%, se considerarmos que todas as certificações partem do setor empresarial. Apenas 13 Estados Membros da UE ultrapassam as 200 certificações. Se nos voltarmos para Portugal, sob análise das mesmas bases de dados e com o mesmo critério de interpretação, de 905 385 empresas ativas (2018), apenas 121 estarão certificadas, o que corresponde a 0.01%. Pelo exposto, a Norma ISO 27001 não denota qualquer relevância para 99.9% do setor empresarial que está vinculado ao RGPD, o que não invalida o seu *compliance*, mas não se faz aproveitar das potencialidades desta padronização internacional.

Concludentemente, ainda que a certificação da ISO 27001 não seja os *standards* de que a implementação do RGPD e o seu estado de conformidade dependam, será de ponderar

[318] Designadamente, o Princípio da Integridade e confidencialidade, com origem na jurisprudência alemã, correspondendo ao "direito fundamental à garantia da confidencialidade e integridade dos sistemas técnico-informacionais" (Grundrecht auf Gewahrleistung der Integritat und Vertraulichkeit informationstechnischer Systeme) – No Acórdão do Tribunal Constitucional Federal (Alemão) de 27 de fevereiro de 2008 – 1 BvR 370/07, disponível em:
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

[319] Consultável em https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Business_demography_statistics#General_overview; https://ec.europa.eu/eurostat/databrowser/view/bd_9bd_sz_cl_r2/default/table?lang=en.

[320] Consultável em: https://www.iso.org/the-iso-survey.html; https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.

uma análise exaustiva dos factos pelos quais se desvalora os padrões internacionalmente reconhecidos, quando a aplicação uniforme, o quanto possível, e por padrão pertencem à razão de ser do Regulamento.

Numa outra dimensão, reitera-se que estamos perante uma área de atuação que exige um amplo conhecimento, qualificações constantes e atualizadas. Os próprios membros do *Ethics Advisory Group* da *European Data Protection Supervisor* (EDPS) – em português, o Grupo de Aconselhamento Ético da Autoridade Europeia para a Proteção de Dados) – representam uma cacofonia de conhecimentos necessários[321] a ter em linha de conta quando estamos perante os Dados Pessoais e a sua necessária proteção, já que desse Grupo Europeu constam filósofos, especialistas em geopolítica do risco, economistas, professores de ética, até mesmo compositores de música clássica. Portanto, a questão das novas tecnologias, da revolução digital e do quanto impactam no epicentro dos nossos valores fundamentais, é uma vertente que não pertence apenas aos especialistas de ciência tecnológica ou de legislação.

Numa listagem de tarefas a cumprir por parte do Encarregado de Proteção de Dados, de tão extensa amplitude, é exigível que a sua seleção seja da mais acertada e prudente possível. É nesta figura, circundada por uma equipa de profissionais de proteção de dados proporcional à dimensão dos dados pessoais a proteger, que as organizações devem apostar em prol da salvaguarda da generalidade dos preceitos legais. Essa aposta exige a disponibilização de recursos imprescindíveis para a concretização das suas funções, nomeadamente as qualificações atualizadas nesta área científica, pelo que não poderá cair na tentação de certificações rápidas e formações definitivas, já que é uma falsa alusão ao que será exigível para o praticante de proteção de dados.

As próprias atividades organizacionais ficarão nas mãos dos gestores de privacidade, não só na relação (com persuasão) dos Responsáveis do tratamento com os subcontratados, mas também com aqueles cujos dados pessoais estejam dependentes da proteção adequada. Toda a relação laboral sairá prejudicada por excesso de zelo ou falta dele, ou até por falta de compreensão dos preceitos gerais das normas *data* protecionistas, acarretando em efeitos prejudiciais nos funcionários, nos colaboradores e nos clientes ou utentes das entidades.

[321] Consoante uma análise do *curriculum* desses membros apresentada por LUÍS ANTUNES, *in Pôr em Prática o RGPD – O que muda para nós? E para as organizações?*, FCA, 2018, pág. XII.

No ponto de vista prático, é clarividente que a realidade nacional ainda está muito distante do que seria expectável aquando da entrada em vigor da norma comunitária. A inexistência de coimas por falta de nomeação do EPD ou por padrões de Segurança de Informação desadequados é questionável. Numa breve pesquisa, tanto no âmbito das PME como na Administração Pública, há ainda quem esteja a iniciar os parâmetros de implementação e até mesmo quem desconheça por completo a existência de nomeação obrigatória de um DPO.

Poderá surgir uma ponderação equilibrada, por parte da Autoridade de Controlo enquanto entidade a quem incumbe o poder sancionatório, entre o que seria exigível às empresas (numa fase de colapso económico à escala mundial) e o que seria exigível em nome dos direitos dos titulares de dados pessoais. Estaremos a dar tempo ao tempo que já foi adiado (passe a redundância).

Por forma a elucidar algumas indicações para futuras investigações na área científica, a solução passará por uma maior aproximação entre a equipa de profissionais de proteção de dados e os titulares dos dados pessoais. Numa outra perspetiva, por uma maior proatividade dos que foram a verdadeira razão da aprovação desta legislação como um normativo dirigido às pessoas e centrado em direitos dos titulares.

Na primeira ponderação, seria vantajosa a concreta identificação do EPD e não apenas do Responsável pelo Tratamento (até mesmo em plataformas ou aplicativos específicos) e que os contactos das equipas de proteção de dados se distanciassem do âmbito interno da organização. Vejamos a necessidade do *DPO* estar acessível aos titulares de dados pessoais. Não implica a partilha de um contacto pessoal, identificável enquanto Pessoa Singular. O contacto tende a ser, por exemplo, privacidade@nomedaentidade.pt, até mesmo para o Encarregados de Proteção de Dados que constituam uma empresa externa, ligada a vários Responsáveis. Tal não invalida que seja considerado como acessível, mas será utópico acreditar que um funcionário da própria organização venha a apresentar dúvidas ou reclamações por intermédio de um correio eletrónico associado à entidade patronal. Estaremos no plano da Política de acesso e do que as Normas ISO 27000 pretendem assegurar, desde logo, a garantia que tal correio eletrónico será passível de ser acedido exclusivamente pelo *DPO* e equipa associada, além dos deveres de sigilo e confidencialidade exigidos. No entanto, para que haja eficácia prática neste caso concreto, pesará a acreditação do próprio

funcionário no sistema, sendo questionável se ficará na mesma posição que outro titular de dados pessoais externo à entidade.

Por outro lado, a proatividade daqueles a quem fica centrada a proteção de dados pessoais é outro ponto a investigar. JOSÉ SARAMAGO, em 1998, no discurso proferido pelo Nobel da Literatura, fez inspirar o documento entregue à ONU, em 2018, por PILAR DEL RÍO. Saramago considerava a Declaração Universal dos Direitos Humanos como algo inacabado e suscetível de ser complementado pela Declaração ou Carta Universal dos Deveres do Homem. Mais do que sermos detentores de direitos, devemos exigir que o cumprimento desses direitos seja efetivo. Os direitos não alcançarão a sua plenitude se não abraçarem a chamada "ética da responsabilidade". Pela descrença na "mão reguladora dos mercados", acredita-se que a titularidade de dados pessoais só ficará salvaguardada quando a parte interessada praticar a responsabilidade social individual, e, assim sendo, só poderá exigir a proteção de dados pessoais quando cumprir com o seu dever de cidadania responsável.

Referências Bibliográficas

Livros:

- ANTUNES, Luís, *Pôr em Prática o RGPD, o que muda para nós? E para as organizações?*, 1ª edição, Lisboa, FCA, 2018;
- ANTUNES, Mário e RODRIGUES, Baltazar*, Introdução à Cibersegurança – A internet, os aspetos legais e a análise digital forense,* 1ª edição, Lisboa, FCA, 2018;
- COUNTINHO, Francisco e MONIZ, Graça (*et alia*) Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2018, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf;
- COUNTINHO, Francisco e MONIZ, Graça (*et alia*) Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2019, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf;
- COUNTINHO, Francisco e MONIZ, Graça (*et alia*) Anuário do Direito da Proteção de Dados Pessoais, CEDIS, 2020, disponível em: https://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf;
- COELHO, Pedro, *Internet das Coisas*, *Introdução prática*, 1ª edição, Lisboa, FCA, 2017;
- CORDEIRO, A. Barreto Menezes – *O Consentimento do Titular dos Dados no RGPD,* 2018, disponível em: https://blook.pt/publications/publication/e772e2d8f7b4/;
- CUNHA, Daniel, HIERRO, Ana e SILVA, Diogo, *Guia do Processo de Adequação ao Regulamento Geral de Proteção de Dados – Implementação e Auditoria*, Coimbra, Almedina, 2020;
- FARINHO, Domingos, *Intimidade da vida privada e media no ciberespaço*, Coimbra, Almedina, 2006;
- FAZENDEIRO, Ana, *Regulamento Geral sobre a Proteção de Dados,* 3ª edição, Coimbra, Almedina, 2018;
- GRANJAL, Jorge, *Segurança Prática em Sistemas e Redes com Linux*, 1ª edição, Lisboa, FCA, 2017;
- HARARI, Yuval, *Homo Deus – História Breve do Amanhã*, 7.ª Edição, Lisboa, Elsinore, 2018;
- MAÇÃS, Fernanda e CALVÃO, Filipa, *O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas – notas breves para a compreensão do seu estatuto*, Fórum de Proteção de dados (CNPD), n.º 07, dezembro de 2020, disponível em: https://www.cnpd.pt/media/5kajlbve/forum7_web.pdf;
- MAGALHÃES, Filipa e PEREIRA, Maria, *Regulamento Geral de Proteção de dados Manual Prático*, 2ª edição, Porto, Vida Económica, 2018;
- PINHEIRO, Alexandre (*et alia*), *Comentário ao Regulamento Geral de Proteção de Dados*, Edições Almedina S.A., 2018;
- RODRIGUES, José e TEVES, Daniela, *A Proteção de Dados Pessoais e a Administração Pública – o novo paradigma jurídico*, AAFLD, 2020;
- SANT'ANA, Simão e GOUVEIA, Vitorino, *O RGPD e os Recursos Humanos – Guia Prático para a conformidade*, Edições Almedina S.A, 2021.
- SALDANHA, Nuno, *Guia para uma auditoria de conformidade – dados, privacidade, implementação, controlo, compliance,* 1ª edição, Lisboa, FCA, 2019;

- SALDANHA, Nuno, *Novo Regulamento Geral de Proteção de Dados – o que é? A quem se aplica? Como implementar?,* 1ª edição, Lisboa, FCA, 2018;
- SILVEIRA, Alessandra, *Princípios de Direito da União Europeia – Doutrina e Jurisprudência,* Lisboa, Quid Juris, 2009;
- SILVEIRA, Alessandra e CANOTILHO, Mariana (*et alia*) Comentário ao Artigo 8.º de CASTRO, Catarina Sarmento, *in* "Carta dos Direitos Fundamentais da União Europeia Comentada", Coimbra, Almedina, 2013.

Legislação, Orientações e Normas ISO:

- Carta dos Direitos Fundamentais da União Europeia;
- Código do Trabalho;
- Código do Procedimento Administrativo;
- Constituição da República Portuguesa;
- Convenção Europeia dos Direitos do Homem;
- Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108);
- Deliberação/2019/495 da CNPD, relativo à solicitação de dispensa de aplicação de coimas às entidades públicas;
- Diretiva n.º 95/46/CE;
- Diretiva n.º 2002/58/CE, relativa à privacidade e às comunicações eletrónicas;
- Diretiva n.º 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicação que altera a Diretiva n.º 2002/58/CE;
- Diretiva n.º 2016/681, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização de dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão de atos terroristas e criminalidade grave;
- ISO/IEC 17021-1 – *Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements*
- ISO/IEC 27000 – *Information Technology – Security techniques – Information Security management systems – Overview and vocabulary*
- ISO/IEC 27001 – *Information Security Management*;
- ISO/IEC 27002:2013 – *Information technology – Security techniques – Code of practice for information sexurity controls;*
- ISO/IEC 27035:2016 – *Information technology – Security techniques – Information security incidente management – Part 1: Principles of incidente management;*
- ISO/IEC 27701:2019 – *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines;*
- ISO/IEC 29100:2011 – *Information technology – Security techniques – Privacy framework;*
- ISO/IEC 29101:2018 – *Information technology – Security techniques – Privacy architecture framework;*
- ISO/IEC 29134:2017 – *Information technology – Security techniques – Guidelines for privacy impact assessment;*

- ISO/IEC 29151:2017 – *Information technology – Security techniques – Code of practice for personally identifiable information protection;*
- ISO/IEC 31000:2018 – *Risk management – Guidelines;*
- Lei n.º 10/91, de 9 de abril – Lei da Proteção de Dados Pessoais Face à Informática;
- Lei n.º 26/2016, de 22 de agosto – Lei de Acesso a Documentos Administrativos;
- Lei n.º 28/94, de 29 de agosto – Aprova Medidas de Reforço da Proteção de Dados Pessoais;
- Lei n.º 43/2004, de 18 de agosto – Lei da Organização e Funcionamento da CNPD;
- Lei n.º 58/2019, de 8 de agosto – Lei de Proteção de Dados Pessoais (assegurou execução do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016);
- Lei n.º 67/98, de 26 de outubro – Lei da Proteção de Dados Pessoais;
- Lei n.º 109/2009, de 15 de setembro – Lei do Cibercrime;
- Lei n.º 145/2015, de 9 de setembro - Estatuto da Ordem dos Advogados (EOA);
- Lei Federal Alemã de Proteção de dados *(Bundesdatenschutzgesetz – BDSG)*;
- Linhas orientadoras do Comité Europeu para a Proteção de Dados Pessoais - Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3º) – *version adopted after public consultation.* Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_pt (consultável a julho de 2021);
- Linhas orientadoras do Comité Europeu para a Proteção de Dados – Diretrizes 7/2020 sobre os conceitos de Responsável e Subcontratado, disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-072020-concepts-controller-and_en;
- Linhas orientadoras do Comité Europeu para a Proteção de Dados - Guidelines 4/2018 on the accreditation of certification bodies under article 43 of the General Data Protection Regulation (2016/679). Annex 1 – version for public consultation. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2018/edpb-guidelines-42018-accreditation_en (consultável a julho de 2021);
- Linhas orientadoras do Grupo do artigo 29.º para a proteção de dados. *Opinião 05/2014 sobre Técnicas de anonimização.* Versão do documento disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf;
- Linhas orientadoras do Grupo do artigo 29.º para a proteção de dados – WP 243 rev.01 (2017). *Orientações sobre os Encarregados da Proteção de Dados.* Versão portuguesa do documento disponível em: https://periciacomputacional.com/wp-content/uploads/2019/05/wp243rev01_pt.pdf (consultável em julho de 2021);
- Linhas orientadoras do Grupo do artigo 29º para a proteção de dados – WP 244 rev.01 (2017). *Orientações sobre a Identificação da Autoridade de Controlo Principal do responsável pelo Tratamento ou do subcontratante.* Versão do documento disponível em: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf (consultável em julho de 2021);
- Linhas orientadoras do Grupo do artigo 29º para a proteção de dados – WP 248 rev.01 (2017). *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o Tratamento é "suscetível de resultar num elevado risco" para*

Efeitos do Regulamento (UE) 2016/679. Versão do documento disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236;
- Linhas orientadoras do Grupo do artigo 29º para a proteção de dados - WP 250 rev.01 (2018). *Guidelines on Personal Data Breach Notification under Regulation 2016/679*. Versão do documento disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052;
- Recomendação CdE sobre a definição de perfis;
- Recomendação CdE sobre os dados estatísticos;
- Regulamento n.º 1/2018 da CNPD relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD)
- Regulamento n.º 45/2001;
- Regulamento n.º1338/2008 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho (JO L 354 de 31.12.200) – definição jurídica de saúde pública, pág. 70;
- Regulamento n.º 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais por autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais;
- Regulamento dos Ensaios Clínicos (UE) n.º 536/2014;
- Regulamento Geral sobre a Proteção de Dados (Regulamento n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados);
- Resolução do Conselho de Ministros nº41/2018, de 28 de março;
- Texto de Substituição da Proposta de Lei n.º 120/XIII/3.ª.

Sítios Web consultados:

- Artigo de ALEX YUMASHEV sobre *Help desk in* Jitbit, 2020, disponível em: https://www.jitbit.com/news/helpdesk-service-desk-itsm/ (consultável a julho de 2021);
- Artigo de CATARINA SARMENTO E CASTRO – *45 anos de "Utilização da Informática" – o artigo 35.º da Constituição da República Portuguesa, in* e-pública — Revista eletrónica de Direito Público, disponível em: https://www.e-publica.pt/volumes/v3n3a04.html (consultável a julho de 2021);
- Artigo de FÁBIO RICARDO DE OLIVEIRA sobre *Service Desk in Movidesk*, 2019, disponível em: https://conteudo.movidesk.com/ferramentas-service-desk/(consultável a julho de 2021);
- Artigo de JE editors e Cegoc *in* Jornal Económico, 2017, disponível em: https://jornaleconomico.sapo.pt/noticias/o-novo-petroleo-sao-os-dados-229587 (consultável a julho de 2021);
- Artigo de JOÃO CAMACHO PEREIRA sobre a exigência multidisciplinar do EPD, *in* Inova Legal, 2020, disponível em: https://inovalegal.org/a-exigencia-multidisciplinar-do-encarregado-de-protecao-de-dados/;

- Artigo de JOSH FRUHLINGER sobre a Fuga de Informação na *Equifax*, *in* CSO, 2020, disponível em: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (consultável a julho de 2021);
- Artigo de KHALED EL EMAM, intitulado por "Does anonymization or de-identification require consent under the GDPR?", *in* IAPP, 2019, disponível em: https://iapp.org/news/a/does-anonymization-or-de-identification-require-consent-under-the-gdpr/.
- Artigo de *The Mind Tools Content Team* sobre Diagrama de *Ishikawa*, 2020, disponível em: https://www.mindtools.com/pages/article/newTMC_03.htm (consultável a julho de 2021);
- Artigo de *The Mind Tools Content Team* sobre Técnica de *Brainstorming*, 2020, disponível em: https://www.mindtools.com/brainstm.html (consultável a julho 2021);
- Base de dados da Eurostat, relativa às empresas ativas em 2018, disponível em: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Business_demography_statistics#General_overview; https://ec.europa.eu/eurostat/databrowser/view/bd_9bd_sz_cl_r2/default/table?lang=en;
- Base de dados da ISO, relativa às certificações ISO/IEC 27001:2013 válidas em 2019, disponível em: https://www.iso.org/the-iso-survey.html; https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1.
- Comissão Europeia em matéria de proteção de dados pessoas: https://ec.europa.eu/info/law/law-topic/data-protection_pt;
- Comissão Nacional de Proteção de Dados (CNPD): www.cnpd.pt;
- Comunicado APDPO relativo à exoneração do EPD da Câmara Municipal de Lisboa, disponível em: https://www.dpo-portugal.pt/noticias/185-tribunal-de-justica-da-uniao-europeia-reforca-poderes-das-autoridades-nacionais-de-protecao-de-dados-2;
- Conselho da Europa: www.coe.int;
- Curso Preparatório para a certificação criado pelo Professor Cláudio Dodt na plataforma Udemy, disponível em: https://www.udemy.com/course/isfs-iso27001/ (consultável a julho de 2021);
- Curso "RGPD para implementadores na Administração Pública", 1ª edição, na plataforma da "NAU – Sempre a Aprender", em parceria com a "INA – Direção-Geral da Qualificação dos Trabalhadores em Funções Públicas, disponível em: https://en-www.nau.edu.pt/course/gdpr-for-implementers-in-public-administration/ (consultável a julho de 2021);
- Definição de Incidente com distinção de acidente, disponível em: https://www.infopedia.pt/$acidente-ou-incidente?uri=lingua-portuguesa/incidente (consultável a julho de 2021);
- Diário da República Eletrónico: www.dre.pt;
- Exemplificação de Gestão da Segurança NOS – Comité de Segurança da Informação multidisciplinar, disponível em :

https://www.nos.pt/institucional/PT/Sustentablidade/atuar/Paginas/Gestao-da-Seguranca.aspx (consultável a julho de 2021);
- Guia de temáticas para a certificação dos Fundamentos Básicos de Segurança de Informação, baseados na ISO/IEC 27001 e 27002 de 2020/2021 disponível em: https://www.exin.com/br-pt/certificacoes/#certifications/information-security-foundation-based-iso-iec-27001-exam(consultável a julho de 2021);
- Guia de Gestão técnica de dados DMBoK2, disponível em: https://www.dama.org/cpages/body-of-knowledge (consultável a julho de 2021);
- Manual da Legislação Europeia sobre Proteção de Dados, disponível em: https://op.europa.eu/pt/publication-detail/-/publication/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1;
- Nota Informativa oficial do caso de fuga de informação da *Equifax*, da *Federal Trade Comission – Protection America's Consumers,* em 2019, disponível em: https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related(consultável a julho de 2021); e em: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement(consultável a julho de 2021);
- Notícia de ERIC NEWCOMER, *in Bloomberg*, sobre ataque informático a dados pessoais (UBER), 2017, disponível https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data(consultável a julho de 2021);
- Parecer n.º 20/2018 (Processo n.º6275/ 2018) sobre a Proposta de Lei n.º 120/XIII/3 disponível em: https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d46446232317063334e686279396a5a57593359544d794f4330325a44526c4c54526c4e546b74596a41304e4331694e54426d4f5449314d6a64684d7a45756347526d&fich=cef7a328-6d4e-4e59-b044-b50f92527a31.pdf&Inline=true;
- Parlamento Europeu: www.europarl.europa.eu/portal/pt;
- Parlamento Europeu (2016). Regulamento n.º 2016/679, de 27 de abril – Regulamento Geral de Proteção de dados. Publicado no *Jornal Oficial da União Europeia* (L 119) em 2016-05-05, pp. 1-88. Versão portuguesa do documento disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT (consultável em julho de 2021);
- PORDATA – Base de Dados Portugal Contemporâneo (2016). *Pequenas e médias empresas em % do total de empresas: total e por dimensão.* Disponível em:https://www.pordata.pt/MicroPage.aspx?DatabaseName=Portugal&MicroName=Pequenas+e+m%C3%A9dias+empresas+em+percentagem+do+total+de+empresas+total+e+por+dimens%C3%A3o&MicroURL=2859&. (consultável em julho de 2021);
- Relatório de atividades de 2017/2018 da CNPD. Disponível em: https://www.cnpd.pt/media/fjhffphw/relatorio_201718.pdf (consultável em julho de 2021);
- Relatório de atividades de 2019/2020 da CNPD. Disponível em: https://www.cnpd.pt/media/adsndrsf/relato-rio-2019-2020.pdf (consultável em julho de 2021);

- SeguraNet – navegar em segurança. Disponível em: https://www.seguranet.pt/ (consultável em julho de 2021).

Jurisprudência:

- Acórdão do Supremo Tribunal de Justiça, de 29 de novembro de 2016, Processo n.º 7613/09.3TBCSC.L1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/-/A4AD03AAA6D934278025807A00589B2F;
- Acórdão do Tribunal Constitucional Federal (Alemão), de 27 de fevereiro de 2008 – 1 BvR 370/07, disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html;
- Acórdão do Tribunal Constitucional n.º 241/02, relatado pelo Conselheiro Artur Maurício (Processo n.º 444/01). Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20020241.html;
- Acórdão do Tribunal Constitucional n.º 255/02, relatado pelo Conselheiro Guilherme da Fonseca (Processo n.º 646/96 e Processo n.º 624/99). Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20020255.html;
- Acórdão do Tribunal Constitucional n.º 355/97, relatado pelo Conselheiro Tavares da Costa (Processo n.º182/97). Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/19970355.html;
- Acórdão do Tribunal Constitucional n.º 403/2015, relatado pelo Conselheiro Lino Rodrigues Ribeiro (Processo n.º 773/15). Disponível em: http://www.tribunalconstitucional.pt/tc/acordaos/20150403.html;
- Acórdão do Tribunal de Justiça da União Europeia UE, de 7 de novembro de 2013, relatado por C. G. Fernlund (Processo n.º C-473/12). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62012CJ0473&from=pt;
- Acórdão do Tribunal de Justiça da União Europeia, de 11 de dezembro de 2014, relatado por M. Safjan (Processo C-212/13). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62013CJ0212;
- Acórdão do Tribunal de Justiça da União Europeia, de 13 de maio de 2014, relatado por M. Ilešič (Processo C-131/12). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0131;
- Acórdão do Tribunal de Justiça da União Europeia, de 16 de julho de 2015, relatado por K. Lenaerts (Processo C-615/13). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62013CJ0615;
- Acórdão do Tribunal de Justiça da União Europeia, de 20 de dezembro de 2017, relatado por M. Ilešič (Processo C-434/16). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62016CJ0434;
- Acórdão do Tribunal de Justiça da União Europeia, de 30 de maio de 2013, relatado por A. Ó Caoimh (Processo C-342/12). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62012CJ0342;
- Acórdão. do Tribunal Distrital de Gelderland (Holanda), 1ª instância, de 13 de maio de 2020 (Processo C/05/368427). Disponível em: https://gdprhub.eu/index.php?title=Rb._Gelderland_-_C/05/368427.