Manuel Ferreira

O Regulamento Geral Sobre a Protecção de Dados

Aspectos legais e organizativos de governança nas organizações

Tese com vista à obtenção do grau de Mestre em Direito e Segurança

Orientador: Doutor Francisco Pereira Coutinho,

Professor da Faculdade de Direito da Universidade Nova de Lisboa

Março de 2018

Manuel Ferreira

O Regulamento Geral Sobre a Protecção de Dados

Aspectos legais e organizativos de governança nas organizações

Tese com vista à obtenção do grau de Mestre em Direito e Segurança

Orientador: Doutor Francisco Pereira Coutinho,

Professor da Faculdade de Direito da Universidade Nova de Lisboa

Março de 2018

Agradecimentos

Num trabalho que visa realçar a protecção de dados, arriscarei, sem o consentimento dos nomeados, agradecer da forma menos intrusiva possível para a privacidade de cada um.

Começo por agradecer aos meus pais, que desde sempre, e em tudo apoiaram-me, mesmo nos momentos em que a nossa opinião divergia, incentivaram-me a seguir os meus objectivos - *"A boa educação é moeda de ouro. Em toda a parte tem valor." (P. António Vieira),* a eles devo a minha educação.

Uma palavra de apreço, ao Professor Francisco Pereira Coutinho, pela orientação e pela disponibilidade demostrada, em todos os momentos da realização desta dissertação.

Aos familiares e amigos, que com amizade e fraternidade, contribuíram positivamente para o meu percurso académico.

Estou especialmente grato ao Sílvio Gomes, pelo seu valioso contributo, pela troca de ideias, pela validação de hipóteses e pelos ensinamentos com candura transmitidos, que muito valorizaram este trabalho.

Por fim agradeço, àqueles que sustentam o meu equilíbrio, e me permitem uma existência alegre e harmoniosa, ao César, Flora e Laura.

"Quando se navega sem destino, nenhum vento é favorável"

Séneca

LISTA DE SIGLAS E ABREVIATURAS

AEPD – Autoridad Española de Protección de Datos

Art. – Artigo

Directiva – Directiva 95/46/CE, de 24 de Outubro de 1995

N.º – Número

p. – Página

pp. – Páginas

UE – União Europeia

EUA – Estados Unidos da América

RGPD – Regulamento (UE) n.º 679/2016, de 27 de Abril de 2016 (Regulamento Geral sobre a Protecção de Dados)

TJUE - Tribunal de Justiça da União Europeia

ISO 27001 – NORMA ISO 27001

Resumo

O Regulamento (EU) 2016/679, sobre a protecção dos dados das pessoas singulares, será directamente aplicável, em todos os estados Membros da União, a partir do dia 25 de Maio de 2018.

Nos últimos tempos, tem sido um dos documentos jurídicos mais referidos e discutidos, nem sempre da forma mais adequada.

O presente trabalho tem como objectivo analisar aspectos fundamentais do referido regulamento tentando contribuir para recentrar o debate, enfatizando as principais alterações do novo regime jurídico sobre a protecção de dados.

Assim, considera-se de primordial importância, identificar e avaliar o impacto que o novo paradigma regulatório introduz na governança das organizações dos sectores público e privado.

Um conjunto de obrigações novas, que densificam o quadro legal existente, terá que responder aos direitos dos titulares dos dados.

As organizações terão que desenhar um sistema interno, com procedimentos e medidas técnicas e organizativas, capaz de demonstrar e de garantir a conformidade com o regulamento europeu.

A nova arquitectura política e organizativa, das entidades públicas e das empresas privadas, terá que ter por base os dois princípios fundamentais que o regulamento coloca no centro das operações de tratamento dos dados pessoais e que são os princípios da finalidade e da necessidade.

Garantido o respeito por estes princípios, existem duas condições essenciais de legitimidade para proceder-se ao tratamento lícito dos dados pessoais que são o consentimento do titular e a existência de enquadramento legal obrigatório.

Como garantia da implementação e da manutenção de uma política e de um sistema de gestão de protecção de dados, aplicando as melhores práticas organizativas, o regulamento criou a figura do Encarregado de Protecção de Dados.

Não sendo de designação obrigatória, o regulamento vê, nesta figura, um "provedor" que garante a continuidade da conformidade demonstrável, em ligação com os titulares dos dados e a Autoridade de Controlo nacional.

Palavras – chave:

Protecção de dados, RGPD, Titulares de dados pessoais, operações de tratamento, EPD, Segurança do Tratamento, Consentimento, Direitos dos Titulares, Autoridade de Controlo, Conformidade, Governança.

Abstract:

Regulation (EU) 2016/679, on the protection of personal data of individuals, is directly applicable in all Member States of the European Union, from 25 May 2018.

In recent times, has been one of the most legal documents referred to and discussed, not always in the most appropriate way.

The present study aims to analyze the fundamental aspects of this Regulation trying to contribute to refocus the debate, emphasizing the main changes in the new legal rules on data protection.

So, it is of paramount importance, identify and assess the impact that the new regulatory paradigm introduces in the *governance* of organizations in the public and private sectors.

A set of new obligations, which consolidated the existing legal framework, will have to respond to the rights of data subjects.

Organizations will have to draw an internal system, with procedures and new organizational measures and techniques, capable of ensuring and demonstrating compliance with the European regulation.

The new political and organizational architecture, public authorities and private enterprises, will have to be based on two fundamental principles that the regulation puts in the center of processing operations of personal data and what are the principles of purpose and necessity.

Guaranteed respect for these principles, there are two essential conditions of legitimacy to be lawful processing of personal data which are the proprietor's consent and the existence of legal framework required.

As a guarantee for the implementation and maintenance of a policy and a data protection system, applying the best organizational practices, the Regulation created the figure of the data protection officer.

Not being mandatory assignment, the regulation sees, in this figure, a "provider" that ensures the continuity of the demonstrable compliance, in conjunction with the data subjects and the national supervisory authority.

Key words:

Data protection, RGPD, personal subjects, data processing operations, EPD, security of processing, consent, rights of personal subjects, Supervisory Authority, Compliance, Governance.

Índice

1. Introdução

A resistência e a dificuldade de adaptação aos avanços tecnológicos, em especial na Era digital, não é uma questão nova. Ao longo da história há vários exemplos de uma certa aversão à novidade, principalmente se isso afectar directamente os nossos hábitos e costumes.

No que concerne à evolução do direito, normalmente, as novas leis percorrem o seu caminho através dos usuais mecanismos da sua feitura, baseadas em fontes do direito tradicionais e de uma paulatina adaptação à própria sociedade.

Os processos de adaptação social acompanham a evolução das necessidades e vão originar as novas normas, que permitem um tempo de adaptação e comunhão com a letra da lei. Este tempo não tem paralelo quando o objecto a regular se prende com os meios de avanço rápido e permanente como sejam a internet ou, de uma forma mais abrangente, o ciberespaço[1].

Por vezes, a agenda política e jurídica não coincidem com a realidade das necessidades. A questão dos perigos no ciberespaço que ameaçam a nossa sociedade, pelo menos há duas décadas, aparece em termos formais na política de segurança nacional e, apenas em 2013, no Conceito estratégico de Defesa Nacional[2] . Este é apenas um exemplo em que vemos de forma

[1] Segundo Pierre Lévy, *Cibercultura, Epistomologia e sociedade*, Instituto Piaget, Lisboa, 2000. p. 16, o ciberespaço é um novo espaço de comunicação proporcionado pela interconexão mundial de computadores e das memórias dos computadores. Incluindo aí todos os sistemas de comunicação electrónica que transmitem informações oriundas de fontes digitais ou que sejam destinadas à digitalização.

[2] Veja-se no documento do conceito estratégico de defesa nacional de 2013, quando refere – "O processo de globalização e a revolução tecnológica tornaram possível uma dinâmica mundial de integração política, económica, social e cultural sem precedentes. Criou um quadro de

notória a necessidade de um tempo de reflexão para se tomar uma decisão sobre as medidas a implementar, de forma a responder a este novo desafio. As questões das ameaças de cibersegurança, são motivo de inquietude por parte dos governos, há já bastante tempo, principalmente após os eventos de ciberataques ocorridos em 2007 e 2008 na Estónia e Georgia[3]. Ainda assim e actualmente continua sem ser uma prioridade na agenda da maioria dos estados.

A informação que é gerada e transferida, a cada segundo no ciberespaço, coloca elevados desafios que, muitas vezes ficam sem solução.
Algo se tem feito, mas muito falta ainda fazer, não obstante, o Direito continua a ser o instrumento preferencial, e talvez o único capaz de no imediato regular a utilização do ciberespaço.

1.1 Âmbito, justificação e objectivos do trabalho

Neste trabalho abordam-se os dados pessoais[4], como um tipo específico de informação, inseridos no novo quadro jurídico da protecção de dados pessoais na União Europeia.

---

interdependência crescente, uma forte tendência de homogeneização e novas condições de progresso. Mas tornaram, também, possível uma difusão equivalente de ameaças e riscos em todas as dimensões, que incluem tanto a projeção das redes terroristas e de crime organizado, como a proliferação das armas de destruição massiva, a fragilização de Estados e o potencial devastador dos ataques cibernéticos" disponível em https://www.defesa.pt/documents/20130405_cm_cedn.pdf, p.12 (consultado em agosto 2017)

[3] Este tema foi alvo de estudo do Eng. Lino Santos no seu trabalho – "*Contributos para uma melhor governação da cibersegurança em Portugal*", Dissertação de Mestrado em Direito e Segurança FDUNL, 2011, onde se pode, de uma forma esclarecida entender o potencial alcance de ciberataques.

[4] Dados pessoais dizem respeito a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»). É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental,

O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados), também conhecido por RGPD vem trazer novas garantias aos titulares dos dados pessoais, através de uma maior protecção no seu tratamento, e um maior controlo por parte do titular sobre os seus dados pessoais, com o reforço dos direitos, que pode exercer, se vir os seus dados tratados de forma ilícita.

O RGPD revoga a Directiva 95/46/CE e trás novas e acentuadas alterações na área da protecção de dados.

A aplicação do RGPD levanta algumas interrogações, enfrenta alguns perigos que importa identificar e corre riscos a avaliar na sua implementação nas empresas. Esta avaliação do risco é um ponto fulcral no entendimento e na operacionalização do RGPD nas organizações. Se observarmos de uma forma atenta, alguns dos principais artigos do regulamento, e mais ainda naqueles que levam à obrigação da implementação de medidas técnicas e organizativas, verificamos uma repetida preocupação da importância da avaliação do risco no tratamento de dados pessoais.

As variáveis: natureza, âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, e ainda a probabilidade e a gravidade a ter em conta nas operações de tratamento de dados a realizar, assumem uma relevância

económica, cultural ou social dessa pessoa singular; definição segundo o Regulamento (UE) 2016/679. Artigo 4º, n.º1.

inquestionável para quem queira garantir a conformidade legal com o RGPD em qualquer organização.

Como peça jurídica nova terá que abrir o caminho que tem que percorrer, sem a ilusão de facilidades.
Muito do que é referido no RGPD, e que terá de obrigatoriamente de levar a uma mudança nas práticas das organizações que tratam dados pessoais, terá de ser gerida numa análise baseada no risco de efectuar esse tratamento.

Assim, entende-se que a grande questão é saber se o RGPD terá a força necessária para gerar o impacto pretendido, e se os principais objectivos do legislador europeu são efectivamente alcançados.

Que desafios e que grau de significância se colocam nas respostas às obrigações deste regulamento? Como estão as organizações dos sectores público e privado a preparar-se para responder e garantir a conformidade com as suas regras? Que incentivos e benefícios podem esperar-se desta conformidade? Concretamente, que papel podem os Encarregados de Protecção de Dados (EPD) desempenhar no seio das organizações, sabendo-se como estas são palcos de tensões conflituantes?

Após o enquadramento do tema em estudo, especificam-se os objectivos deste trabalho, a saber:

- Identificar as principais alterações políticas e jurídicas na protecção de dados do RGPD, relativamente à Directiva 95/46/CE;

- Compreender o Impacto e os desafios que estas alterações poderão ter nas organizações;

- Dar a conhecer as principais medidas técnicas e organizativas que os responsáveis pelo tratamento de dados pessoais têm que adoptar para alcançarem a conformidade com os princípios jurídicos da protecção de dados;

- Compreender a importância da figura do Encarregado da Protecção de Dados, e o seu contributo para a governança da protecção de dados nas organizações.

Por impulso do RGPD, a protecção de dados pessoais está na ordem do dia, obrigando a uma abordagem totalmente diferente daquela a que estamos acostumados. Olhar os dados pessoais como um direito fundamental e com liberdade de circulação controlada, e não como mera mercadoria em mercado desregulado, acarreta desafios civilizacionais significativos para as organizações, em especial na definição da sua política e governança em matéria de protecção de dados pessoais.

Assim, partilha-se com a comunidade científica a pertinência de estudar estes desafios que o RGPD vem colocar às sociedades.

De acordo com os objectivos supramencionados, esta tese foi estruturalmente organizada em sete capítulos.

No primeiro capítulo, expõem-se os objectivos do trabalho, as questões a investigar, e traça-se um enquadramento geral do tema em apreço.

No segundo capítulo refere-se a evolução do conceito da protecção de dados, desde os seus primórdios até ao regulamento 2016/679, passando pela Directiva. Nas várias subsecções deste capítulo, procura-se traçar um quadro geral do RGPD, passando pelo princípio da responsabilidade demonstrável, conforme especificado no número dois do artigo 5.º do RGPD, sendo aplicável a todos os aspectos da conformidade até aos procedimentos a implementar. Realiza-se ainda, uma análise aos direitos do titular, enfatizando o papel de um dos mais relevantes princípios da protecção de dados, chegando à análise de um dos principais fundamentos de legitimidade para tratar dados pessoais, como é o consentimento.

No terceiro capítulo, pretende-se analisar e perceber os diversos níveis de responsabilidade, de maturidade e de preparação dos vários *stakeholders* com impacto na governança da protecção de dados nas organizações. Referem-se também, alguns aspectos relacionados com a actuação espectável da autoridade de controlo, dos tribunais, dos titulares dos dados, e dos subcontratantes, salientando-se todo o quadro sancionatório e não só, os valores definidos para sancionar quem não cumpra com o RGPD. Rejeita-se o recurso a este argumento do terror, como abordagem adequada às sanções.

O capítulo quatro, é dedicado à segurança da informação. Aí, realiza-se um estudo comparativo entre os requisitos da Norma ISO 27001 e as medidas técnicas e organizativas exigidas pelo artigo 32º do RGPD, relativo à segurança no tratamento. São ainda descritas as obrigações do responsável pelo tratamento, onde se insere a protecção de dados desde a concepção e

por defeito, a avaliação de impacto de protecção de dados, a notificação de incidentes, e a consulta prévia à autoridade de controlo.

A figura do Encarregado de Protecção de dados é referida no capítulo cinco, onde se realiza uma análise às responsabilidades e às garantias associadas ao desempenho desta função, salientando-se o papel deste profissional no seio da organização como garante da conformidade do RGPD.

O último capítulo é reservado às conclusões que se consideram mais relevantes, apresentando-se o resultado final do estudo feito nesta dissertação.

1.2 Enquadramento do tema

Cada vez mais se verifica, a par dos avanços tecnológicos com as consequentes questões levantadas nessa "alucinação consensual diariamente experimentada por biliões de operadores legítimos, em cada país"[5], onde faltam respostas céleres e com enquadramento legal.

As inovações tecnológicas estão a obrigar, cada vez mais, a um esforço e agilidade na produção jurídica que, muitas vezes, não acompanha a velocidade dos acontecimentos.

As normas jurídicas, bem como o seu processo clássico de elaboração com base na jurisprudência, nos costumes, ou na doutrina, bem como em outras fontes do direito, encontram sempre dificuldades e resistências de adaptação, relativamente às novas tecnologias.

Não é a primeira vez que a humanidade se depara com avanços tecnológicos. Retrocedendo até ao início da Era da Revolução Industrial, encontra-se o movimento ludita[6], que se opunha à mecanização do trabalho, principalmente devido à incerteza provocada pelo desconhecido, e pela alteração do modo de vida e de sustento dos trabalhadores.

[5] Gibson, William, *Neuromante*, Gradiva, Lisboa, 2004, p.53, citação retirada da citada obra, em que Gibson considera o ciberespaço uma alucinação consensual diariamente experimentada por biliões de operadores legítimos, em cada país, por crianças a quem são ensinados conceitos matemáticos... Uma representação gráfica de dados extraídos de bancos de cada computador do sistema humano. Complexidade impensável.

[6] Ludismo ou movimento ludita é o nome dado a um movimento ocorrido na Inglaterra entre os anos de 1811 e 1812, que reuniu alguns trabalhadores das indústrias contrários aos avanços tecnológicos em curso, proporcionadas pelo advento da primeira revolução industrial. Os ludistas protestavam contra a substituição da mão-de-obra humana por máquinas.

O impacto que teve a rápida transformação dos processos produtivos originou uma resposta negativa nas pessoas que eram directamente afectadas por estas inovações, gerando-se violentas resistências e barreiras à nova realidade.

Actualmente, na maioria dos sectores de actividade também se assiste a uma resistência à mudança. Quanto à protecção de dados nota-se um enorme desinteresse na maioria das empresas privadas e dos organismos públicos.

Este desinteresse dificulta a adopção das novas obrigações de protecção de dados, vindas à luz com o RGPD.

Estes “neoluditas” são os primeiros grãos na engrenagem, que terão de ser sensibilizados e consciencializados para reconhecerem a importância do tratamento de dados pessoais, de acordo com os requisitos legais do Regulamento 2016/679, e assim prepararem a empresa para o mercado, já apelidado por muitos como o novo petróleo, que são os dados pessoais. Sobretudo pelas potencialidades em termos de proveitos comerciais que podem advir da manipulação e tratamento deste tipo de informação, como é exemplo a definição de perfis ou da análise de metadados.

Os desafios imediatos que o RGPD coloca também devem ser vistos numa perspectiva a longo prazo. Nesse sentido, exige-se uma atitude pró activa de gestão da mudança, contra o conformismo e o imobilismo organizacional.

Urge caminhar para uma mudança. Para tal é necessário ambicionar uma alteração de paradigmas internos nas organizações, sabendo que apenas se

poderá alcançar os resultados de uma mudança, se juntarmos o desejo de gerar essa mudança ao esforço de a gerir.

"Para sobreviver e ter sucesso, cada organização tem de se tornar um agente da mudança. A forma mais eficaz de gerir a mudança é criá-la."[7]

Os esforços que as organizações estarão disponíveis a fazer para se adaptarem ao requerido pelo RGPD estará directamente relacionado com o conhecimento das matérias sobre a protecção de dados que consigam adquirir.

Os conhecimentos relativos à protecção de dados, combina vários campos do saber. Quem ambicionar manter-se actualizado e conhecedor dos avanços da segurança da informação e da protecção de dados terá que estar em sintonia, quer com os avanços tecnológicos, quer com as leis relativas à regulação do ciberespaço, do comércio electrónico, ou à segurança de redes informáticas, etc.

Da mesma forma, os avanços da Internet, a facilidade de transferência de grandes quantidades de informação para qualquer parte do mundo e de forma quase instantânea, acarreta enormes desafios para quem pretende regular o ciberespaço onde tudo acontece.

[7] Nas palavras de Peter Drucker, *Desafios da gestão para o século XXI,* Livraria Civilização Editora, 2000,p.114, em que o autor afirma que "*a melhor forma de gerir a mudança é criá-la*". Pode fazer-se uma associação desta ideia às alterações organizativas que o RGPD obrigará nas empresas, tendo cada uma, que adaptar-se à mudança, para poder sobreviver e ter sucesso.

Recentes tecnologias e novas formas de tratar grandes quantidades de dados, vem possibilitando todo um novo espectro de utilizações e interconexões de informação que produzem resultados muitas vezes inesperados, e nem sempre positivos.

Entrou no nosso léxico o termo *Big Data*[8], que se pode considerar como uma tecnologia para processar um elevado volume de dados, que são gerados no ciberespaço a grande velocidade. Através de algoritmos de *data mining,* podem correlacionar-se e analisar-se enormes quantidades de informação, tirando disso proveitos de vária ordem. A definição de perfis é um exemplo que pode obter-se através da análise de *big data,* e que desta forma permite inferir as preferências de um individuo, ou grupos de indivíduos.

Como anteriormente referido, nem sempre este tipo de tecnologia é utilizado com fins claros e favoráveis aos titulares de dados.

Uma mesma tecnologia que utilize um algoritmo que possa ajudar numa simples pesquisa do voo mais barato para certo destino, pode da mesma forma ser utilizada para o recolher os dados das pessoas e categorizar o seu perfil, e com isso segmentar uma categoria ou grupo de utilizadores, para direcionar mensagens sobre questões que interessam (a cada grupo), usando linguagem e imagens que as possam gerar

[8] O big data refere-se a dados que podem ser recolhidos de uma forma massiva, e analisados computacionalmente, com o intuito de identificar padrões, preferências e tendências relacionadas, entre outros, com um negócio ou actividade.

"engagement" (compromisso), e dessa forma induzir tendências e influenciar as decisões de um individuo.

É neste contexto que surge o RGPD, com um conjunto de obrigações para os responsáveis pelo tratamento, que o torna um passo importante para a regulação do tratamento e livre circulação dos dados das pessoas singulares, e que este, possa criar um ponto comum de debate no seio da EU para alavancar a construção (na medida do possível), de um mecanismo de regulação do ciberespaço.

Um espaço dificilmente mensurável, mas que todos reconhecemos como imenso e incerto, onde circula enormes quantidades de informação, marcando uma Era a quem já muitos identificaram como a Era da informação.

Um bom exemplo é a obra "A terceira vaga" [9],onde Alvin Toffler nos dá um vislumbre ficcional do que poderia ser o futuro, com a chegada da Era da Informação.

Apesar da obra referida ter o seu enfoque principal na economia, é fácil compreender que se atingiu o que Toffler designou de "sobrecarga da informação", bem como a dependência da tecnologia em vários sectores.

Concomitantemente, com o volume de informação digital que é hoje partilhado e com a facilidade de, em qualquer parte do planeta e através de diversos meios, surgem diariamente novas utilizações do ciberespaço.

[9] Toffler, Alvin, *A Terceira vaga*, 1.ª edição, vida e cultura, Lisboa, 1984.

Se por um lado isto proporcionou-nos vários ganhos e facilidades a diversos níveis, também passou a ser um meio perigoso, propício à criminalidade de vários tipos, e, portanto, um espaço crítico a controlar e a legislar.

Mas quais são os limites admissíveis? Quanto da nossa liberdade e privacidade estamos dispostos a ceder, para que a nível estatal ou supraestatal, como é o caso da UE, possa ser-nos dada uma garantia de segurança no ciberespaço? Como garantir, ao mesmo tempo, a segurança física, a privacidade, a protecção de dados, a inviolabilidade do domicílio e da correspondência como prevê a nossa Constituição?

Segurança ou privacidade, ou porque não os dois? Ao que parece não é uma equação fácil de resolver. Neste contexto assume particular relevância a ideia de Ulrich Beck: "A sociedade moderna tornou-se uma sociedade de risco, uma vez que debate cada vez mais os riscos que ela própria criou, para os controlar e impedir." [10]

Em 2013, assistimos a um episódio, que ganhou contornos de escândalo mundial, quando se soube que o governo federal dos EUA fazia um rastreio ilegal e indiscriminado, aos conteúdos de ligação, aos emails e às mensagens trocadas nas redes sociais, através do programa de vigilância "*Prism*"[11], criado durante a administração de George W. Bush.

[10] Beck, Ulrich, *Sociedade de risco mundial, em busca da segurança perdida*, Edições 70, Lisboa, 2015, p. 103.

[11] Este programa secreto, foi tornado publico pela mão de Edward Snowden, que forneceu documentos pormenorizados, ao jornal The Guardian, em que revelava o modo de funcionamento do programa Prism.

O presidente Obama declarou, no seguimento destes acontecimentos e em jeito de justificação, que "não é possível garantir cem por cento de Segurança com cem por cento da privacidade."[12]

O programa *Prism* recolhia metadados[13]. Em Portugal, a recolha do mesmo tipo de informação foi negada ao SIRP (Sistema de Informações da República Portuguesa), pelo Tribunal Constitucional[14], a possibilidade de acederem a estes dados para a persecução das suas atribuições. No entanto, os metadados de muitos portugueses foram analisados e utilizados pelo programa *Prism*, evidenciando uma vez mais as dificuldades de regular equitativamente e de forma global o ciberespaço.

Vê-se alguma incoerência, no pouco cuidado com que os metadados são tratados de forma massiva por parte das instâncias judiciais em Portugal. A directiva 2006/24/CE[15], invalidada pelo Tribunal de Justiça da União Europeia (TJUE), no conhecido caso *Digital Rights Irland[16],* acabou por ser

[12] Declarações do Presidente Barack Obama, vídeo disponível em, https://youtu.be/KVY3mq6B-5w (consultado em Dezembro de 2017).

[13] Segundo a definição avançada no acórdão 403/2015 do tribunal constitucional, n.º 773/15,Conselheiro Lino Rodrigues Ribeiro.
disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20150403.html (consultado em dezembro de 2017) - Metadados é Informação estatística não visível, respeitante a um determinado documento, gerada por um programa de software.

[14] O acórdão 403/15, n.º 773/15 cit. considera que o acesso aos metadados por parte do SIS e do SIED, viola o artigo 34º, n.º 4 da Constituição da Republica Portuguesa - É proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal.

[15] Directiva 2006/24/CE do Parlamento europeu e do conselho de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE.

[16] Decisões do TJUE Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, C-288/12 - disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1536533157417&uri=CELEX:62012CA0293 (consultado em setembro de 2017)

transposta para a Lei 32/2008, que continua a produzir efeitos, permitindo a conservação de metadados no âmbito da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Admitamos que o estado da arte não permite grande ambição a este respeito, e que a segurança tenha um pendor mais relativo. Admitamos ainda que o tema é discutível, podendo desenvolver-se uma argumentação de ambos os lados do binómio segurança/privacidade.

No entanto, exige-se que os avanços na segurança não sejam à custa da privacidade, e que a regulação necessária assente no desenvolvimento de tecnologias controláveis e não intrusivas dos direitos à privacidade, à reserva da vida privada, à intimidade e a outros valores civilizacionais já vertidos em vários documentos nacionais e internacionais.

É conveniente e esperado que não se entre numa espiral de mediatismo e de alarmismo, que não raras vezes culmina em leis, que podem colocar em perigo princípios e direitos que foram paulatinamente conquistados desde os finais do século XIX, época de Warren[17] e Brandais[18], quando surge pela primeira vez e de forma estruturada o conceito de *privacy*[19] nos EUA.

[17] Samuel Dennis Warren (1852 – 1910). Formado em Harvard. Editor da revista *Harvard Crimson*.[Warren e Brandeis fundaram um escritório de advocacia de Boston, Nutter McClennen & Fish em 1879. No final de 1890, publicou seu famoso artigo de opinião jurídica,"*O Direito à Privacidade*" na revista *Harvard Law Review*.

[18] Louis Dembitz Brandeis (1856 –1941) foi um advogado Norte-Americano e membro do Supremo Tribunal dos Estados Unidos entre 1916 a 1939. Formado em Direito na Universidade Harvard, com a média de notas mais alta na história da faculdade até então.

[19] Decidiu-se pelo termo em inglês, precisamente para marcar a diferença entre o conceito *privacy* nos Estados Unidos da América, e o conceito de privacidade nos termos da carta dos direitos fundamentais da União Europeia.

Quando ocorrem calamidades públicas ou ataques terroristas, que causam pânico e consternação generalizada, é importante que não se adoptem leis reactivas[20], muitas vezes com efeitos nefastos para a privacidade, direitos e liberdades dos cidadãos.

Pelo exposto, considera-se fundamental que as forças cívicas e a opinião pública dos países democráticos continuem alerta, e façam ouvir as suas vozes vigilantes para poderem responder em conformidade quando confrontados com atropelos aos mais essenciais direitos já conquistados.

Esta tarefa cívica é, em primeira mão, dos políticos e da Justiça. Na verdade "quando a legislação tem falhado, têm sido os tribunais nacionais e internacionais a reencaminhar as soluções para a rota dos direitos fundamentais"[21].

[20] USA Patriot Act é um bom exemplo de uma "lei reactiva", aprovada logo após os atentados de 11 de setembro 2001, por George W. Bush. Esta lei vai permitir que órgãos de segurança e de inteligência dos EUA, designadamente a NSA, interceptem ligações telefónicas e e-mails de organizações e pessoas supostamente envolvidas com o terrorismo, sem necessidade de qualquer autorização da Justiça, sejam elas estrangeiras ou americanas.

[21] Pinheiro, Alexandre Sousa - *Privacy e Protecção de Dados Pessoais*: *A Construção Dogmática do Direito à Identidade Informacional*, AAFDL, Lisboa, 2015, p.118

2. Evolução da protecção de dados

2.1 Privacy e protecção de dados

Não sendo o objectivo deste trabalho identificar e avaliar as diferenças entre os conceitos de *privacy* na perspectiva americana do termo, e de protecção de dados na visão europeia, pretende-se, ainda assim e de forma resumida, abordar o que está na origem destes dois conceitos distintos, e como podemos, actualmente, identificar cada um deles.

O conceito de privacidade, como é hoje conhecido, tem a sua origem nos EUA, nos finais do século XIX por Warren e Brandeis, através do conhecido artigo "The Right to Privacy"[22].

Nesse artigo os seus autores colocaram em evidência a ocorrência de transformações sociais, políticas e económicas, bem como o surgimento de novas invenções, como a fotografia, como factores que contribuíram para a ocorrência de violações da vida privada das pessoas".
Pode considerar-se esta a primeira Era da *privacy*[23], que surge com o elemento disruptivo que é a captação da imagem pela primeira máquina fotográfica Kodak.

[22] "The Right to Privacy" é um artigo jurídico escrito por Samuel Warren e Louis Brandeis, publicado em 1890 na revista *Harvard Law Review*. Disponivel em: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (consultado em Janeiro 2018)

[23] Pinheiro, Alexandre Sousa - *Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional*, cit., p.277.

Já no século XX surgiu na Alemanha o conceito de *Datenschutz*[24] o mais aproximado ao nosso actual conceito de protecção de dados, que corresponde à segunda Era, tendo como elemento tecnológico de base, o processamento de dados pessoais por computador.

A terceira Era chegou com o advento da Internet – Web2.0 e Web 3.0, tendo por base o elemento tecnológico de suporte ao fluxo de informação brutal que gerou.

Com a evolução da internet e com todas as suas possibilidades, em especial com o aparecimento do direito à identidade informacional[25] – conceito diferente do da privacidade como "direito à autodeterminação informativa", o qual concede a cada um de nós um real poder sobre as nossas próprias informações e sobre os nossos próprios dados.

Na evolução do conceito de privacidade, desde a originária definição – *the right to be let alone* –, chega-se até ao desenvolvimento conceptual elaborado por Stefano Rodotà[26] como sendo o direito de manter o controlo sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada.

[24] Tradução directa do Alemão – *Datenschutz* – Protecção de dados. Um documento essencial para percorrer os primórdios do conceito de *Datenschutz*, é analisar o parecer de um grupo de especialistas liderado por Wilhem Steinmüller em 1972 sobre a *Datenschutz* e a *informationelle Selbstbestimmung*, disponível em https://edoc.hu-berlin.de/bitstream/handle/18452/6063/59.pdf?sequence=1 (consultado em Março de 2017).

[25] Resultante do conceito do "direito a ficar só", ou direito à vida privada concebido por Robert Kerr quarenta anos antes de Warren e Brandais.

[26] Rodotà, Stefano, *El derecho a tener derechos*, trotta, Madrid, 2014, p.84

Neste âmbito, configura-se o direito à privacidade como um instrumento fundamental contra a discriminação e a favor da igualdade e da liberdade.

Com efeito, as sociedades de informação, como são as sociedades em que vivemos, pode dizer-se que "nós somos as nossas informações"[27], pois são elas que nos definem, que nos classificam, que nos etiquetam.

Aqui entra-se no âmago das questões da privacidade como sejam o controlo da circulação das informações e o conhecimento sobre a identidade de quem as usa, o que significa adquirir, concretamente, um poder sobre si mesmo. Pode considerar-se que o conceito de privacidade está ligado aos princípios da dignidade humana e do direito à reserva da vida privada e da intimidade, enquanto o conceito da protecção de dados, remete-nos para uma ideia de direito, uma garantia da nossa identidade informacional, e o nosso controlo sobre a mesma.

No ponto seguinte, o trabalho desenvolve-se sobre a temática da protecção de dados, conforme expressa no regulamento 2016/679 do Parlamento Europeu e do Conselho, no alinhamento com o objecto de estudo da segurança e da protecção dos dados das pessoas singulares.

[27] *Idem*

2.2 O Regulamento Geral sobre a Protecção de Dados

Considerações Gerais

Desde 2012, aquando da apresentação da primeira versão da proposta regulamento, que se iniciou um amplo e complexo debate entre os países membros da União, com uma forte participação de grandes empresas multinacionais.

Verificou-se então uma actividade de lobby muito intensa, para limitar a extensão e a profundidade das exigências legais do regulamento, associada a outras posições resultantes de diferentes graus de sensibilidade e de maturidade, na abordagem do tema sobre a protecção de dados, reflectindo desiguais desenvolvimentos nas políticas e nas práticas dos Estados-Membros da UE.

Foi neste contexto agitado e complexo, com diversos contributos, com diversas pressões e exigências nacionais, corporativas ou outras, que se desenrolou o processo de negociações e compromissos para a aprovação final de um texto com aplicação obrigatória em todos os Estados-Membros.

Considerando o objecto, o objectivo e o âmbito territorial de aplicação entende-se que algum grau de generalização e de abstracção teria que percorrer o regulamento.

No entanto, e numa leitura atenta aos 173 considerandos que enquadram os 99 artigos que compõem o regulamento, é possível identificar algumas incongruências no seu articulado e alguns conceitos vagos e indeterminados.

Existem também muitas remissões para o direito interno, o que dá alguma margem legislativa aos Estados-Membros.

Em resumo, pode considerar-se que o regulamento expressa uma política de compromisso entre os vários interesses nacionais e corporativos, presentes no tabuleiro do tema da protecção de dados, o que determinou um texto final denso e complexo. Apesar do difícil processo de gestação, pode realçar-se o facto de que hoje poucos colocam em causa a importância e a projecção presente e futura do RGPD.

Entende-se que, ao capacitar as empresas para a garantia da protecção e da livre circulação dos dados das pessoas singulares, se vive uma grande oportunidade de preparar as organizações para o grande mercado dos dados.

2.2.1 O RGPD e os organismos públicos

Uma das questões deixada em aberto pelo RGPD é saber se as coimas serão ou não aplicadas aos organismos públicos[28].

O regulamento deixa a cada Estado-Membro a decisão final em causa própria. Possibilita uma saída jurídica, que beneficie os organismos públicos, salvaguardando-os da eventual aplicação de coimas, criando um ambiente mais “relaxado” que o vivido pelo sector privado.

[28] Pode ler-se no Art. 83º, n.º 7 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que, sem prejuízo dos poderes de correcção das autoridades de controlo nos termos do artigo 58.º n.º 2, os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território.

Admite-se que esta situação, a verificar-se, venha a criar uma desigualdade entre os sectores público e privado, prejudicial à credibilidade dos propósitos enunciados no regulamento.

O Estado-Membro que seguir essa via, que se considera facilitista, deixa a fiscalização à aplicação do regulamento numa situação de fragilidade e de manifesta desautorização, podendo abrir caminho para enfraquecer, senão mesmo para esvaziar, a importância da Autoridade de Controlo.

Pelo exposto, e admitindo-se outras opiniões, entende-se ser fortemente recomendável que cada Estado-Membro seja o primeiro a dar o exemplo do cumprimento de todos os requisitos vertidos no regulamento para a protecção dos dados pessoais dos cidadãos. Pode mesmo dizer-se que em todos os Estados-Membro da União são os organismos públicos os que mais dados de pessoas singulares tratam, incluindo as categorias especiais de dados.

A aprovação e a publicação das diversas iniciativas legislativas, em curso em vários parlamentos europeus, vão dizer muito sobre o sentido que os Estados-Membros dão à protecção de dados.

2.2.2 Algumas ideias correntes sobre o RGPD

Em Portugal, país sem tradição política e cultura cívica sobre a privacidade e a protecção de dados, vai-se ouvindo as mais díspares interpretações sobre o tema, as mais infundadas esperanças sobre os “benefícios” de alguma inoperância fiscalizadora, etc.

No entanto todas têm um traço comum, a saber: desconhecimento e desvalorização do regulamento e do seu impacto nas organizações, crença na inactividade da Autoridade de Controlo, margem temporal para ver o que vai passar-se e alguma fé no recurso à litigância judicial para contestar eventuais decisões sancionatórias, entre outras ideias.

No presente trabalho considera-se o regulamento da maior importância, independentemente dos seus aspectos mais críticos. Entende-se mesmo que é um novo marco na forma como doravante vamos olhar para os titulares dos dados e a importância acrescida dos cuidados a ter com os dados das pessoas singulares.

2.3 Directiva vs Regulamento

Alguma confusão vai existindo sobre as diferenças conceptuais entre uma Directiva e um Regulamento. Verifica-se, até de quem não se espera, um uso indiferenciado dos termos, pelo que se exige uma clarificação da terminologia que anda pelas bocas do nosso mundo.

Um dos equívocos mais comuns em torno do RGPD é considera-lo como se de uma directiva se tratasse. Esperam alguns que “saia a sua “transposição” para então se fazerem ao caminho. Nada mais erróneo.

Um «Regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE, não carecendo de transposição para a ordem jurídica nacional. Tem um carácter geral e é obrigatório em

todos os seus elementos e directamente aplicável em todos os Estados-Membros (art. 288.º do Tratado sobre o Funcionamento da União Europeia).

Uma directiva é um ato legislativo que fixa um objectivo geral que todos os países da UE devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objectivo (art. 288.º do Tratado sobre o Funcionamento da União Europeia).

A verdade é que, independentemente de existir ou não uma nova lei interna sobre a protecção de dados, a partir de Maio de 2018, todos os requisitos e obrigações legais que constam do RGPD, têm impreterivelmente que ser cumpridas.

Cada Estado-Membro pode, e diga-se deve, definir com maior pormenor o que o RGPD deixa em aberto, ser mais preciso onde se verifica alguma incerteza, densificando zonas e intervalos largos para algumas decisões.
Por exemplo, no capítulo das sanções, o RGPD define os valores máximos a aplicar, mas não os valores mínimos, nem valores intermédios, com alguma proporcionalidade face ao nível sancionatório considerado adequado de acordo com a constatação a sancionar.

2.4 Demonstração da responsabilidade

Seguramente uma das principais alterações é a maneira como as organizações terão que estar preparadas para responder às exigências do RGPD, principalmente no respeitante à resposta a dar ao artigo 5º n.º 2.

O responsável pelo tratamento é o responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).

O nº 1 do art. 5.º refere-se aos princípios que devem orientar qualquer operação de tratamento de dados pessoais a realizar por um responsável.

Este deve garantir em todos os momentos e iterações com dados pessoais, a sua licitude, lealdade e transparência, de acordo com as finalidades do tratamento, tendo em conta os limites da conservação, a minimização dos dados e assegurando simultaneamente a exactidão, a integridade e a confidencialidade dos dados tratados.

Com a entrada em aplicação do RGPD, todos os princípios referidos assumem uma importância fulcral nas operações de tratamento de dados. Como decorre do artigo 5º, nº 2, o responsável pelo tratamento, além de ter que cumprir com todos os princípios enunciados, tem que conseguir comprová-lo.
Para comprovar o cumprimento dos requisitos do regulamento, as empresas têm que elaborar um conjunto de documentos que indiquem os procedimentos a seguir e os registos associados[29]. Ou seja, têm que criar

[29] Artigo 30º, n.º1, do RGPD: Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. O Registo das atividades de tratamento é obrigatório para empresas com mais de 250 trabalhadores.

evidências para todas as operações de tratamento realizadas, quer por meios automatizados, quer não automatizados[30], de forma a poder demonstrar que todas as operações de tratamento realizadas cumprem com os princípios enunciados no RGPD.

É importante ter em atenção que uma organização que cumpra com os requisitos legais do Regulamento, mas não tenha forma de demonstrar que o faz, é, para todos os efeitos, considerada em falta para com as normas instituídas e está, desta forma, sujeito a sansões por parte da autoridade de controlo.

2.5 Da hetero-regulação para a auto-regulação

Do ponto de vista operacional, a exigência de ter de comprovar a conformidade com o regulamento muda toda a forma de encarar a problemática da protecção de dados dentro das organizações.

Até Maio de 2018, a protecção de dados foi regulada numa perspectiva de hétero-regulação, em que a necessidade de garantir a licitude do tratamento, através dos princípios e condições de legitimidade, ocorria essencialmente na fase inicial, pelos meios definidos pela autoridade de controlo (notificação,

[30] Artigo 5°, n.º 2, do RGPD: Tratamento - uma operação ou um conjunto de operações efectuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

uma licença ou autorização, por exemplo). Após a entrada em aplicação do RGPD, estamos perante uma nova realidade.

O responsável pelo tratamento tem que conseguir garantir, em qualquer momento do processo de tratamento de dados pessoais, a sua licitude e cumprimento com o RGPD, criando evidências para que o possa comprovar, ficando assim sujeito à fiscalização e supervisão da autoridade de controlo, no nosso caso a Comissão Nacional de Protecção de Dados (CNPD).

É uma alteração significativa na maneira de tratar os dados pessoais dentro das organizações, quer no sector público quer no sector privado, onde o pendor dos sistemas de gestão da protecção de dados terá que estar direccionado para a demonstração da conformidade com o RGPD. Este carácter da "responsabilidade demonstrável" está patente em várias partes do regulamento, seja nos considerandos, seja no articulado principal. Podemos encontrar esta necessidade de demonstrar a conformidade com o RGPD nos seguintes considerandos e artigos do RGPD: Considerandos 81, e 85, e artigos 7º, 12º, 24º, 28º, 40º, 42º, apenas para referir alguns.

É por demais evidente que este será um dos elementos mais relevantes, no momento de uma hipotética fiscalização. Estar seguro dos seus procedimentos e registos internos, que evidenciem boas práticas de protecção de dados e da segurança da informação no tratamento de dados pessoais, é o objectivo de qualquer organização em conformidade e capaz de a demonstrar.

2.6 Ferramentas para demonstrar a conformidade com o RGPD

Como referido anteriormente, a questão da demonstração da conformidade com o regulamento, bem como das boas práticas respeitadas no tratamento de dados pessoais, serão motivo de grande relevância, na medida em que apenas podendo demonstrar, se considera em conformidade.

Para tal, o RGPD dá-nos alguns instrumentos, que poderão ser um precioso auxílio nesta tarefa da demostração, entre outros os códigos de conduta, as certificações, marcas e selos, o registo das actividades de tratamento realizadas com dados pessoais, ou as avaliações de impacto de protecção de dados.

Uma das componentes mais ambiciosas do RGPD diz respeito ao Comité Europeu para a Protecção de Dados.

O Comité poderá emitir orientações e pareceres vinculativos, relativamente a um conjunto de situações que a autoridade de controlo de cada Estado-Membro, isoladamente, não poderá fazer. Esta atribuição do Comité constitui um importante contributo para os mecanismos de cooperação, de coerência e de assistência mútua. Este comité poderá ter uma acção fundamental na uniformização de certificações e de códigos de conduta, que uma vez mais, podem servir de meios de prova para demonstrar o cumprimento com o disposto no RGPD.

Os códigos de conduta[31] podem ser utilizados com os seguintes propósitos, a saber:

- Realizar o tratamento de dados, de forma equitativa e transparente;
- Acautelar, em contextos específicos e em determinados sectores de actividade, os legítimos interesses dos responsáveis pelo tratamento;
- Auxiliar na definição dos meios de recolha, a pseudonimização, a resposta aos direitos dos titulares e às obrigações do responsável pelo tratamento;
- Fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou Organizações Internacionais.

O processo de aprovação destes códigos de conduta tem um ciclo próprio.

Numa primeira fase é a autoridade de controlo do Estado-Membro, em que o código de conduta é proposto, que tem que se pronunciar, dando um parecer sobre a conformidade do projecto apresentado.

Numa segunda fase, a autoridade de controlo encaminha-o para o Comité que, por sua vez, dá o seu parecer sobre a coerência e a conformidade nos Estados-Membros da UE.

Numa terceira e última fase, e se o parecer for favorável, a Comissão, através de actos de execução, decide da aprovação dos códigos de conduta e publicita-os. O responsável pela compilação, e disponibilização ao público pelos meios que considere adequados é, uma vez mais, o Comité.

[31] Artigo 40.° do RGPD - Secção 5 - Códigos de conduta e certificação.

A supervisão dos códigos de conduta é feita, em primeira análise, pela autoridade de controlo competente em matéria de protecção de dados. No entanto, esta pode acreditar organismos que demonstrem competência na matéria, e que cumpram critérios rigorosos de independência. As outras autoridades ou organismos públicos é-lhes vedada esta possibilidade.

No caso português será à CNPD, ou à autoridade de controlo que venha a ser constituída, que corresponderá a tutela destas questões.

Para garantir a coerência nestes processos, a autoridade de controlo competente apresenta os projectos de critérios para a acreditação ao Comité, o que permite que não sejam aprovados códigos de conduta com orientações dissonantes em diferentes Estados-Membros, sobre o mesmo sector de actividade. Assim evita-se por em causa um dos princípios fundamentais deste regulamento, que é a procura de uma aplicação homogénea das regras da protecção de dados em toda a UE.

Os códigos de conduta poderão ter uma relevante importância sobre as medidas e as boas práticas no tratamento de dados pessoais a adoptar em micro, pequenas e médias empresas, contribuindo para a demonstração da conformidade com o RGPD. Poderão ainda contribuir para a avaliação de riscos e dos potenciais impactos em determinadas operações de tratamento, que, caso contrário, provavelmente não teriam capacidade nem recursos internos para uma correcta implementação do RGPD.

Em associações ou representantes de categorias de responsáveis pelo tratamento ou subcontratantes, com características especificas de alguns sectores de actividades, é fortemente aconselhável incentivar a elaboração destes códigos de conduta[32].

Está ainda previsto que, para além de podermos utilizar um código de conduta, como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento, pode também ser um meio importante para os responsáveis pelo tratamento e os subcontratantes que não estejam sujeitos ao RGPD, poderem realizar transferências de dados pessoais para países terceiros.

[32] Nos termos do considerando (98), do RGPD, as associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do presente regulamento, com vista a facilitar a sua aplicação efetiva, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares.

2.7 Direitos dos titulares dos Dados

A aprovação da lei 67/98 transpôs para a ordem jurídica portuguesa a directiva europeia 95/46/CE, sobre a protecção de dados das pessoas singulares, defindo um conjunto de direitos dos titulares, que se recordam na Figura 1, a seguir apresentada.

Figura 1 – Direitos dos titulares dos dados especificado na lei 67/98.

O RGPD prevê novos direitos para os titulares dos dados e reforça as obrigações dos responsáveis pelo seu tratamento para assegurar um maior nível de protecção e de controlo dos seus dados pessoais.

Na Figura 2, que a seguir se apresenta, realçam-se os direitos novos no conjunto dos direitos passíveis de serem exercidos pelos seus titulares.

Figura 2 – Conjunto dos direitos dos titulares dos dados especificado no RGPD.

Para além dos direitos já previstos na lei de protecção de dados 67/98, como sejam o direito ao acesso e à rectificação, o direito à informação e à transparência surgem com o novo regulamento, um conjunto de novos direitos, a saber: o direito de portabilidade dos dados (Artigo 20° - RGPD), o direito de oposição (Artigo 21° - RGPD) , o direito à não sujeição a decisões individuais automatizadas, incluindo a definição de perfis (Artigo 22° - RGPD) e o direito ao apagamento (Artigo 17° - RGPD).

Como pode constatar-se, parte dos direitos anteriormente referidos, já estavam consagrados na directiva 46/95/CE, que por sua vez foi transposta para a lei nacional 67/98.

Assim, seria espectável, que esses direitos já estivessem perfeitamente consolidados, e que as organizações estivessem preparadas para responder a qualquer titular dos dados que quisesse exercer esses mesmos direitos, o que de uma forma generalizada hodiernamente não acontece.

Na grande maioria das organizações, o exercício de “direitos antigos”, é um fenómeno alienígeno, estranho, como se nunca tivessem existido.

Por isso, também as organizações evidenciam as mais diversas dificuldades para estudar e entender o RGPD, identificar o seu impacto, conceber a sua implementação, definir o seu enquadramento e acomodamento organizativo e, em especial, perceber a figura do Encarregado de Protecção de Dados. Tudo é uma novidade geradora de estranheza e de desconforto, de custos “desnecessários” e de ameaças.

Estas dificuldades sentem-se nas abordagens realizadas com quadros dirigentes de organismos públicos e de empresas privadas. Ouvem-se em acções de formação sobre o tema. As sanções, enquanto argumento do terror, são o aspecto do RGPD que mais sobressaltos causam.

Antes de se analisarem os vários direitos dos titulares, é importante realçar que estes direitos, como todos, não permitem um exercício absoluto. A este propósito, pode citar-se o considerando (4) quando refere que “O direito à protecção de dados pessoais não é absoluto: deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade”.

O responsável pelo tratamento tem que fornecer ao titular as informações de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, tal como, facilitar o exercício dos direitos do titular dos dados, sem demora injustificada - um mês a dois meses[33].

As informações são fornecidas pelo responsável pelo tratamento, a título gratuito, salvo se os pedidos foram infundados, excessivos e reiteradamente repetidos. Nestes casos pode haver lugar à recusa do pedido, ou à cobrança de uma taxa, por custos administrativos, ao titular dos dados.

Caso o responsável invoque o carácter infundado e excessivo do exercício de um direito, tem que provar que assim é, correndo o risco de uma sanção, se não houver uma justificação plausível.

Por isso, estão previstas situações, em que tais direitos podem ser limitados, ou mesmo recusados, tendo em conta o contexto, e as finalidades para as quais são tratados os dados. Designadamente quando estejam em causa, princípios de liberdade de expressão e de informação, ou exista uma obrigação legal, ou ainda situações envolvendo assuntos de interesse público no domínio da saúde pública, os titulares dos dados podem ver atenuado a possibilidade de exercer os seus direitos em matéria de protecção de dados.

Exceptuando os casos atrás referidos, os titulares dos dados têm à sua disposição, um conjunto de direitos, vertidos no RGPD, que devem ser exercidos de forma informada e consciente.

[33] Artigo 12º , do RGPD

Veja-se então o caminho dos direitos no “mapa” do RGPD.

- **Direito de não sujeição a decisões automatizadas**

O titular dos dados passa a ter o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afecte significativamente de forma similar.

Actualmente é comum, cada vez que se consulta um site na internet, que seja gerado um perfil de preferências dos internautas, com base nos campos consultados, nas pesquisas efectuadas, ou nas compras realizadas.

Este processo de definir os perfis dos titulares de dados é, na maioria das vezes, automaticamente realizado através de algoritmos que calculam e registam dados pessoais de forma pré-definida, sem o consentimento do titular. Neste sentido o direito supramencionado obriga a que o responsável pelo tratamento obtenha o consentimento do titular para proceder ao tratamento dos seus dados pessoais pela forma descrita.

- **Direito de Portabilidade dos dados**

O exercício deste direito tem alarmado muitos responsáveis pelo tratamento, na medida em que pode obrigar à implementação de um conjunto de medidas técnicas, nem sempre possíveis de alcançar com a rapidez e a eficácia pretendidas.

Em algumas situações pode admitir-se que, mesmo havendo uma razoável capacidade técnica e financeira, pode não ser realizável num curto espaço de tempo. Os desafios técnicos para dar resposta a este direito podem gerar alguma dificuldade de concretização.

O RGPD refere que o titular dos dados tem o direito de receber os seus dados num formato estruturado, de uso corrente e de leitura automática, pelo que todas as organizações deverão preparar-se para cumprir com estes requisitos.

- **Direito ao Apagamento**

Por vezes referido como o "direito ao esquecimento", é um direito que permite, aos titulares dos dados, solicitar o apagamento dos seus dados tratados por uma determinada organização.

A possibilidade de exercício deste direito ficou particularmente conhecida, após uma demanda em tribunal por parte de um cidadão de nacionalidade espanhola. Ousou solicitar o apagamento da informação relativa à sua pessoa, que estava indexada no motor de busca da Google, com *links* para anúncios publicados no jornal *La Vanguardia,* relativamente a dívidas que em tempos tivera, mas que no momento da queixa já estavam devidamente regularizadas.

No célebre Acórdão, conhecido por Google Spain[34] , o Tribunal de Justiça da União Europeia (TJUE) veio dar razão ao Sr. *Mario Costeja González* decretando o apagamento dos referidos dados do motor de busca da Google.

[34] Acordão do TJUE, de 13 de Maio de 2014, Google Spain, C-131/12, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1536533544734&uri=CELEX:62012CA0131 (consultado em janeiro 2017)

Antes de mais, deve referir-se que este tipo de informação, trate-se ou não de dados pessoais, mas que esteja indexada em alguns dos vários motores de busca disponíveis, jamais será possível garantir que sejam efectivamente apagados para sempre.

No caso exemplificado, o queixoso conseguiu o objectivo de que se ordenasse a desindexação do conteúdo do seu índice e a impossibilidade de futuro acesso no mesmo motor de busca. Mas nada garante que alguém que tenha recolhido essa informação previamente não a venha a difundir depois pelas inúmeras plataformas disponíveis no ciberespaço. É comum ouvir-se que “uma vez na internet, para sempre na internet”. De facto é impossível eliminar o rasto deixado na internet.

Outro aspecto que deve ser salientado neste caso, é a repercussão que este tema e a sentença associada tiveram no mundo em geral e na Google em particular.

Após a publicação do Acordão do TJUE, a Google foi inundada de pedidos de apagamento, mesmo sem razão aparente, ficando a ideia para muitos, de que os direitos previstos no RGPD possam ser exercidos em qualquer circunstância. Muitos dos titulares que pediram o apagamento dos dados, obrigaram a uma resposta por parte do responsável pelo tratamento. E este, para poder responder, teve que receber o pedido, abrir um processo, analisá-lo, fundamentar e finalmente responder. Trata-se de obrigações, deveras trabalhosas, provocando uma densificação de processos burocráticos com os inerentes custos administrativos associados ao processo de gestão dos pedidos dos titulares.

Admite-se que, com o nível de consciencialização e o desconhecimento existente por parte de muitos dos titulares dos dados, os direitos ao dispor sejam exercidos sem avaliarem se são ou não exigíveis no contexto. Por isso, é recomendável que todas as organizações consigam munir-se de processos e de critérios claros para responderem a um crescimento espectável dos pedidos abusivos para o exercício dos direitos e do aumento da litigância judicial.

2.8 Livre circulação dos dados

Atentando-se ao título do regulamento 2016/649, verificamos que além de focar a sua preocupação na protecção dos dados e do seu tratamento faz-se referência à livre circulação desses dados.

Como vimos anteriormente, as leis de protecção de dados actualmente em vigor nos vários Estados-Membros da UE são fruto da transposição da Directiva 46/95/CE. Cada Estado-Membro elaborou a sua lei interna sobre a protecção de dados das pessoas singulares, resultando assim uma variedade e disparidade de regras e de normas desiguais nos vários países da UE.

Esta situação tem originado algumas dificuldades no que diz respeito à transferência de dados pessoais entre países da União porque, devido a um ordenamento jurídico diferente, geram-se situações em que a mesma operação de tratamento de dados pessoais possa simultaneamente ser considerada lícita num Estado-Membro e ilícita em outro.

A desigualdade de situações pode ser particularmente complexa e problemática em multinacionais ou grupos empresariais que tenham estabelecimentos em vários Estados-Membros da UE, que se vêm até agora na contingência de ter que organizar os seus processos no que respeita à transferência de dados pessoais considerando as diferenças legislativas existentes entre o país de origem e de destino desses dados.

O facto de o RGPD ser de aplicação directa em todos os Estados-Membros, a partir de Maio de 2018, faz com tenhamos as mesmas regras e garantias de protecção de dados, sendo assim possível garantir um nível mais coerente e homogéneo nas actividades e meios de tratamento, e concomitantemente na sua circulação pelos países sujeitos ao cumprimento do regulamento.

2.9 Consentimento

O consentimento é uma das formas que habilita o responsável pelo tratamento a realizar as operações de tratamento de dados pessoais de um titular de forma lícita.

A principal novidade do RGPD está precisamente no momento da concordância do titular dos dados, e acima de tudo na necessidade do consentimento ter que ser dado mediante um acto positivo e claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito[35].

[35] Considerando (32) do RGPD

Mais uma vez o responsável pelo tratamento tem que conseguir demonstrar que, no acto do consentimento, este foi cedido segundo as regras anteriormente referidas, quer tenha ocorrido através de uma declaração escrita, oral ou em formato electrónico.

O facto de, doravante, o consentimento não poder ser assumido de forma tácita, comumente praticado até à data, através do conhecido “quadrado”, em que nos é dada a opção de que os nossos dados não sejam tratados se assinalarmos com um “X”, e que por omissão se nada for assinalado, os dados poderiam ser licitamente tratados, vai deixar de ser possível.

As implicações práticas destas alterações podem afectar sobremaneira as organizações que construíram ao longo do tempo, bases de dados através do consentimento tácito, o que contrariará a letra do RGPD.

As empresas que queiram garantir que podem continuar a utilizar as suas bases de dados após 25 de Maio de 2018, devem fazer um esforço no sentido de que estas sejam adaptadas às novas regras do consentimento explícito, para não correrem o risco de verem impossibilitado o tratamento futuro dos dados pessoais aí registados.

O consentimento assume um papel central na protecção de dados. É o princípio fundamental que permite, em todas as circunstâncias, que o tratamento de dados pessoais de um titular seja lícito, desde que este tenha sido concedido nas condições especificadas no RGPD.

É, no entanto, garantido ao titular de dados a qualquer momento, a possibilidade de este reverter a sua decisão, e retirar o consentimento. Também este facto pode provocar dificuldades por parte do responsável pelo

tratamento, na gestão das bases de dados e sistemas de gestão de dados pessoais, que normalmente não estão preparadas para responder a esta exigência. Todo o tratamento de dados pessoais de um titular, que num determinado momento deu o seu consentimento, e posteriormente o retire, este facto não invalidade a licitude do tratamento até então.

3. Aplicabilidade do RGPD – Quem está preparado para o RGPD?

Desde 27 de Abril de 2016, data da publicação do Regulamento 2016/679 do Parlamento Europeu e do Conselho, que, uma das questões mais colocadas, foi sobre a aplicabilidade do RGPD, em especial o conjunto de obrigações dos responsáveis pelo tratamento, no âmbito da protecção de dados das pessoas singulares.

De que forma as organizações estão preparadas para este desafio, como podem preparar-se e que incentivos terão para levar a sério este regulamento?

Alguns cedo perceberam que poderia estar aqui um novo mercado, com muitas oportunidades para o sector da advocacia, da consultoria de sistemas e das empresas de tecnologias.

De um modo geral, tem sido notório a falta de técnicos qualificados para poder apoiar e auxiliar as organizações a alcançarem a tão desejada conformidade com o RGPD.

Na ausência de critérios “certificadores” de competência nesta área e no contexto de um mercado novo em crescimento acelerado e algo ansioso,

tem-se verificado a emergência de alguns “técnicos”, que exibem competências difíceis de provar, como cosmética para disfarçar a falta de credibilidade profissional e, assim, parasitarem o mercado das “necessidades”.

Numa primeira fase, os escritórios de advogados rapidamente se posicionaram para prestar os serviços necessários para que as empresas estivessem preparadas e a salvo de pesadíssimas coimas. Este movimento trouxe, numa segunda fase, algumas empresas de Tecnologias de Informação, com soluções de suporte desmaterializado para garantir a segurança da informação.

No quadro geral dos contributos de várias áreas, e face às inquietações de algumas organizações (por onde começar?) admite-se que a área da consultoria e de implementação de sistema de gestão pode também contribuir na procura de soluções adequadas ao melhor acomodamento e incorporação da protecção de dados na vida das organizações. Pode ainda ajudar na concepção e na implementação de um sistema coerente e robusto, capaz de fornecer soluções políticas e organizativas consistentes, para a garantir a conformidade da protecção de dados com o RGPD.

3.1 Sanções

Os valores das sanções a aplicar, para quem incumpra as regras do RGPD, são deveras alarmantes, quando comparados com o anterior regime, passando de números de ordem de grandeza dos milhares para os milhões, incluindo também a possibilidade de uma coima calculada com base no volume total da facturação anual de uma empresa, podendo aqui atingir os

4% do volume anual de negócios[36]. Para além das coimas monetárias, a autoridade de controlo pode ainda determinar a cessação de tratamento de dados pessoais a título temporário ou definitivo. Mais uma vez podemos constatar a manifesta intenção do legislador europeu em garantir que todas as organizações, públicas e privadas encarem a protecção de dados como um assunto sério a tratar na agenda de prioridades.

Quanto a este ponto, muito haverá a dizer, e ainda que seja prudente não fazer um exercício de adivinhação, é nossa opinião que as sanções máximas serão aplicadas de uma forma excepcional e em situações por demais evidentes e em incumprimento grave e claro do RGPD, e principalmente a grandes empresas multinacionais, até porque na aplicação destas sanções serão de uma forma proporcionada à gravidade, a natureza, os danos produzidos, e ao número de titulares afectados. No entanto, seja qual for o valor da sanção aplicada neste novo regime jurídico terá valores até à data pouco comuns nestas matérias.

[36] Artigo 83º, n.º5 do RGPD – "A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial corres pondente ao exercício financeiro anterior, consoante o montante que for mais elevado."

3.2 O papel das autoridades de controlo

A autoridade de controlo em Portugal, responsável por controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei, é a Comissão Nacional de Protecção de Dados (CNPD) [37].

A CNPD é uma entidade administrativa independente, com poderes de autoridade, que, salvo alguma alteração a decidir pelo parlamento, poderá continuar a garantir que as empresas privadas e os organismos públicos estejam em conformidade com as leis que digam respeito à protecção de dados pessoais.

Desde 1994 que a CNPD tem tido um papel algo passivo, e por vezes meramente reactivo, centrando a sua actividade na resposta às notificações dos responsáveis pelo tratamento.

As empresas, que pretendam obter autorização ou apenas informar que vão realizar determinada operação de tratamento de dados pessoais, comunicam a sua intensão à CNPD e pagam a taxa estabelecida, sabendo que na grande maioria das vezes o processo fica concluído por aqui.

[37] A Comissão Nacional de Protecção de Dados é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República.
Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei.
A Comissão é a Autoridade Nacional de Controlo de Dados Pessoais.
A CNPD coopera com as autoridades de controlo de proteção de dados de outros Estados, nomeadamente na defesa e no exercício dos direitos de pessoas residentes no estrangeiro. Disponível em www.cnpd.pt/bin/cnpd/acnpd.htm (consultado em abril de 2017).

Ora, no meio deste processo burocrático de análise da legalidade dos pedidos dos responsáveis pelo tratamento e da cobrança das respectivas taxas, a CNPD, tem evidenciado algumas fragilidades, admite-se que por insuficiência de meios humanos e materiais, ficando normalmente por cumprir uma outra importante atribuição[38] de uma autoridade de controlo – o exercício do poder de fiscalização.

Numa leitura atenta do relatório de actividades de 2016[39], pode perceber-se as dificuldades que esta autoridade de controlo tem enfrentado desde há muito.

Com os desafios que o novo quadro jurídico coloca e as dificuldades decorrentes de significativas limitações financeiras, provocadas pelo fim da cobrança das taxas dos registos e pelas restrições orçamentais, o reforço de meios para acompanhar as novas obrigações regulatórias de fiscalização é mais difícil.

[38] São atribuições da CPND (segundo a Lei n.º 43/2004 de 18 de Agosto, Lei de organização e funcionamento da CNPD):
- Controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais.
- Emitir parecer prévio sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos comunitários ou internacionais relativos ao tratamento de dados pessoais.
- Exercer poderes de investigação e inquérito, podendo para tal aceder aos dados objeto de tratamento.
- Exercer poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais.
- Advertir ou censurar publicamente o responsável do tratamento dos dados, pelo não cumprimento das disposições legais nesta matéria.
- Intervir em processos judiciais no caso de violação da lei de proteção de dados.
- Denunciar ao Ministério Público as infrações penais nesta matéria, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de provas.

[39] Disponível em www.cnpd.pt/bin/relatorios/anos/Relatorio_2016.pdf, (consultado em Abril de 2017)

Não havendo um sinal claro por parte do Estado, que quer dotar a Autoridade de Controlo dos meios necessários ao desempenho das suas funções, ficará mais difícil atrair quadros técnicos à altura dos novos desafios.

Admite-se que possa estar um pouco comprometida a resolução de problemas resultantes da carência de quadros da CNPD com um nível de especialização adequado às necessidades actuais e futuras, com competências em várias áreas envolvidas na protecção de dados, tais como o direito, as tecnologias da informação, a segurança de redes informáticas, a segurança da informação, as noções de gestão e de administração de sistemas, e outras.

Como referido anteriormente, a alteração do modelo regulatório, de hétero-regulação para a autorregulação, trará profundas alterações na forma de actuação da CNPD, sendo exigível uma maior actividade fiscalizadora, em contraste com o perfil até agora exibido.

Numa simples operação de cálculo, pode verificar-se que, a CNPD deixa de ter o trabalho administrativo que advém das autorizações e registos das notificações, ficando com os recursos humanos existentes mais disponíveis para a actividade fiscalizadora. A perda de receitas por deixar de cobrar taxas será compensada com uma parte das receitas resultantes da aplicação de coimas.

Pelos sinais emitidos pela CNPD, em especial pela sua presidente Dr.ª Filipa Calvão, através de vários órgãos da comunicação social[40], entende-se que

[40] *"Pode acontecer que a CNPD considere suficiente, depois de uma fiscalização, fazer recomendações ou uma admoestação. Mas sim, também serão aplicadas as sanções previstas na lei" – Dr.ª* Filipa Calvão, Presidente da CNPD (Negócios, 29.01.2018) – disponível em https://www.pressreader.com/portugal/jornal-de-negócios/20180129/281552291292942 (consultado em fevereiro de 2018)

há disponibilidade para marcar presença, com os meios que tiver, na fiscalização da conformidade dos organismos públicos e das empresas privadas face ao RGPD.

Admite-se ainda que a fiscalização será equilibrada e ponderada, face ao comportamento e ao grau de conformidade atingido pelas organizações. Umas vezes a fiscalização terá um pendor mais pedagógico e outras mais sancionatório. Mas tranquiliza os titulares dos dados saberem que vai haver fiscalização.

Assim, é espectável que se inverta a tendência referida no relatório de actividades de 2016, sobre o decréscimo das acções inspectivas realizadas, com a aplicação de coimas com valores tendencialmente mais elevados.

Em 2016 a CNPD aplicou um total de 256 coimas com um valor médio por coima de €1.900,00, aproximadamente.

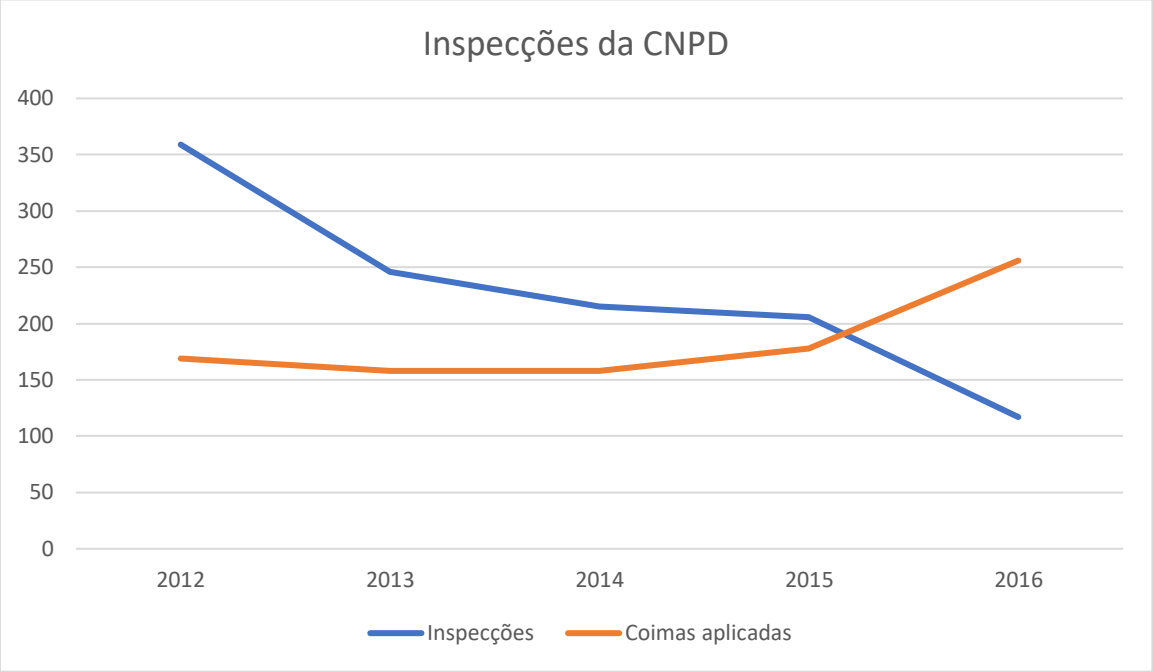

Gráfico 1 – Número de inspecções vs Coimas aplicadas

3.3 Acesso à justiça

O acesso à justiça, principalmente a possibilidade de um titular de dados fazer valer os seus direitos perante um tribunal, sai reforçado com o RGPD.

Ao contrário do estabelecido atualmente, um titular de dados que considere que os seus dados pessoais foram tratados de forma ilícita, fora do seu país, pode intentar uma acção judicial no Estado-Membro da sua residência. Deixa de ter que se deslocar ou eleger um representante no Estado-Membro da sede do estabelecimento do responsável pelo tratamento em questão, contra quem quer intentar a acção de defesa dos seus direitos.

Voltando ao exemplo já dado anteriormente e referente à participação do queixoso no caso Google/Spain para garantir que a poderosa Google apagava os seus dados pessoais (inexactos), teve que intentar uma acção

judicial junto do Estado-Membro que alberga a sede desta empresa em solo europeu, neste caso a Irlanda.

Como é facilmente aceite, nem todos os titulares teriam a capacidade, quer financeira quer jurídica, para enfrentar a maior empresa do mundo no conhecido caso Google Spain.

Cada titular de dados, que veja os seus dados pessoais tratados ilicitamente, passa a poder exercer os seus direitos de uma forma mais fácil, mais célere, e consequentemente menos onerosa.

3.4 Consciencialização dos titulares

Uma das maiores dificuldades será conseguir a alteração da forma de encarar a pertinência da protecção de dados e das práticas fora dos direitos dos titulares e das obrigações referidas no RGPD.
Alterar os paradigmas que têm feito escola constitui o maior desafio das organizações. É sobretudo uma questão de gestão da mudança de mentalidades e de comportamentos associados, pela consciencialização para a problemática que importa proteger com este documento jurídico – as pessoas.

Primeiro, temos o facto de que ninguém dedicou nenhuma atenção à anterior legislação europeia. O impacto que a directiva 95/46/CE teve no tecido empresarial português é no mínimo irrisório, tornando o RGPD uma grande revolução para muitos, quando na verdade grande parte dos princípios jurídicos, as condições de legitimidade para o tratamento de dados, e mesmo os direitos dos titulares, estavam já consagrados da directiva de 1995.

O que acontece é que muito poucos se preocuparam em adoptar as melhores práticas de protecção de dados que a lei 67/98 de protecção de dados que vigora em Portugal desde 1998 já define com grande pormenor.

Nunca houve, no nosso país, uma verdadeira consciência por parte dos titulares de dados, da relevância e da importância que os seus dados pessoais têm, e os prejuízos que podem ser causados se o seu tratamento for descuidado e abusivo. Não há ninguém que não tenha sido pelo menos uma vez na vida, alvo de uma campanha de marketing agressivo. No entanto, a maioria das pessoas não conhece os mecanismos que tem ao seu dispor para combater essa situação.

É notória a diferença de maturidade em Portugal, em termos de consciência no que se refere à protecção de dados, quando comparada com outras realidades como por exemplo a Alemanha.

Este será um caminho que terá de ser percorrido pelos titulares de dados, concomitantemente à evolução dos vários actores e sujeitos jurídicos envolvidos, tais como as autoridades de controlo, os organismos públicos, as empresas privadas, e a respectiva cooperação europeia no seio do comité para a protecção de dados. Apenas o empenho destes vários stakeholders envolvidos, poderão fazer com que os dados pessoais passem a ser vistos como algo de singular importância, e de inestimável valor, num mundo cada vez mais transparente e indiscreto.

Obviamente que o titular não tem apenas direitos, nem estes são absolutos, como já se referiu. É de fundamental importância que cada um compreenda que a protecção principia no momento da cedência dos dados. Quando são fornecidos dados pessoais para um determinado fim, o titular deve

compreender completamente as finalidades para as quais está a dar o seu consentimento. Se por um lado, a lei indica-nos que o responsável pelo tratamento apenas pode processar os dados para as finalidades consentidas e estabelecidas inicialmente, o titular dos dados, por sua vez, tem que compreender que os dados que fornece, sem conhecer as finalidades, poderão pôr em risco a sua protecção, por vezes, com repercussões impossíveis de controlar.

Uma tendência actual e com crescimento acentuado é a quantidade de informação, na maioria dados pessoais, que são diariamente expostos e tornados públicos através das redes sociais, sem qualquer escrúpulo ou hesitação, onde tudo é partilhado online, sem sabermos quem acede a esta informação do outro lado, é no mínimo intimidante.

3.5 Subcontratação

Um subcontratante[41], pessoa singular ou colectiva, que trate dados pessoais por conta do responsável pelo tratamento destes, é autonomamente responsabilizável se incumprir as regras do RGPD.

Num futuro bem próximo e, contrariamente ao previsto na directiva 95/46/CE, sempre que um subcontratante viole alguma das normas da protecção de dados, pode ser responsabilizado, e portanto, alvo de coimas ou de outro tipo de sansões se este determinar as finalidades e os meios de tratamento.

[41] Artigo 4.º do RGPD – Definições 8)

Vários são os casos, ao longo dos últimos anos, em que um subcontratante por incúria, não velava pelos interesses e garantias dos titulares de dados, sabendo que não poderiam ser punidos por tal comportamento despreocupado e, por vezes, negligente.

Importa referir que este tipo de práticas terá um enquadramento jurídico drasticamente diferente, ao ponto de um titular de dados prejudicado por um tratamento ilícito dos seus dados, poder pedir uma indeminização ao responsável pelo tratamento e a um subcontratante, inclusive aos dois se houver eventuais danos causados cumulativamente por estes.

Doravante o tratamento em subcontratação terá necessariamente que ser regulado por contrato ou por outro ato normativo, que vincule o subcontratante ao responsável pelo tratamento, e que estabeleça ainda o objecto, a duração, a natureza e a finalidade do tratamento, o tipo de dados pessoais e as categorias dos dados dos titulares, as obrigações e os direitos do responsável pelo tratamento[42].
A conformidade do subcontratante com o RGPD terá que estar evidenciada num contrato escrito.

A obrigatoriedade de regular a subcontratação em ruptura com os moldes anteriormente definidos, tem outras consequências para o responsável pelo tratamento. Este só poderá recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de modo a que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados[43].

[42] Artigo 28º do RGPD
[43] Artigo 28º do RGPD

4. Segurança da Informação

Como já foi referido, ao longo do presente trabalho, a quantidade de informação gerada e transmitida a cada segundo no ciberespaço, mesmo regulando, protegendo e limitando a sua circulação não deixará de constituir um enorme desafio, transmitir essa informação pela internet e conseguir garantir a sua segurança.

Um campo de estudo que cresce, lado a lado com as necessidades e desafios da internet, é a segurança da informação, que pode ser definido, como o processo de proteger a informação das ameaças, para garantir a sua integridade, disponibilidade e confidencialidade[44].

Numa rede de informação é praticamente impossível seguir-lhe o rasto, momento a partir do qual, será para sempre uma incógnita os caminhos percorridos por essa informação.

Esta nova capacidade de transmissão de informação veio trazer à nossa realidade vantagens evidentes que todos saudamos e agradecemos. Mas também é fácil concordar que "a tecnologia é um promotor da igualdade de oportunidades, proporcionando às pessoas poderosas ferramentas para os seus próprios objectivos"[45] sejam eles bem ou mal-intencionados.

É precisamente para as situações com pendor malicioso que nos temos de preocupar. É fundamental entender que é imperioso garantir a segurança da

[44] Beal, Adriana, *Gestão Estratégica da Informação*, Atlas, Brasília, 2008, p.19.

[45] Eric Schmidt & Jared Cohen – *A Nova Era Digital – Reformulando o futuro das pessoas, das nações e da economia*, D.Quixote, 2013, Lisboa, p. 185.

informação quer no domínio estritamente pessoal e doméstico, quer a nível profissional e em todas as organizações, sejam elas da administração pública, IPSS´s, associações profissionais ou outras, empresas privadas, ou outras.

Hoje em dia é consensual que um arquivo com documentos em papel, que constitua um activo valioso para uma organização, seja alvo de um cuidado especial. Por exemplo, uma sala de arquivo com chave, terá que ter os acessos definidos e controlados, ou se guardada num cofre, a combinação de acesso terá que ser conhecida da(s) pessoa(s) que for(em) definidas superiormente.

Com a informação digital, muitas vezes os cuidados não são os mesmos e muitas vezes não existe sequer a percepção dos riscos que acarretam determinados comportamentos no mundo digital que, mesmo fora da rede, podem originar graves quebras de segurança e de violação de dados, também conhecidos como *data breaches*[46].

Os *data breaches* são muitas vezes potenciados por más práticas e por displicência comportamental, natural em quem nunca foi sensibilizado para os possíveis danos que podem causar aos seus negócios.

No que concerne à segurança no tratamento de dados pessoais, estamos uma vez mais perante um quase de total desconhecimento das obrigações

[46] Data breach – Violação de dados pessoais - uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, definição segundo o RGPD, artigo 4.º (12).

legais. Continua a existir uma grande indiferença quanto ao tratamento de dados pessoais com garantias de confidencialidade, integridade e exactidão dos dados tratados.

Os fluxos deste tipo de informação não são alvo de qualquer medida para assegurar a segurança nas operações de tratamento realizadas, e é bastante comum, em qualquer tipo de organização, que o correio seja triado pelo funcionário que estiver na secção de recepção ou expedição.

É prática corrente o correio ser aberto indiferenciadamente e reencaminhado posteriormente para os respectivos departamentos, sem qualquer controlo dos dados que circulam à merce do acesso, de qualquer funcionário, sejam eles do seu interesse profissional, ou não.

Muita desta informação circulante nada tem de confidencial ou crítica, mas entre o que tem pouca relevância no tocante à protecção de dados encontramos um abundante manancial de dados pessoais, e por vezes dados sensíveis que circulam desprotegidos por várias mãos até chegar ao destino, a quem realmente tem que ter essa informação e proceder ao tratamento dos dados.

4.1 A Segurança do tratamento

Temos referido, ao longo deste trabalho, que o regulamento não é totalmente inovador do ponto de vista das obrigações legais, como é muitas vezes e erradamente apresentado.

Há artigos do regulamento que, ainda que em texto subtil, vão obrigar a significativas mudanças de práticas no tratamento de dados pessoais. É o caso do artigo 32º que se irá agora comentar.

Artigo 32º do RGPD
n.º1 -Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

a) A pseudonimização e a cifragem dos dados pessoais;

b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Entende-se que este artigo vai obrigar a implementar novas medidas e obrigações, assim como outras preocupações organizativas que, não sendo novas, revestem-se de carácter obrigatório em todas as empresas e organismos públicos que tratem dados pessoais, com uma incidência importante sobre os dados tratados por meios informatizados. Como é do conhecimento geral, os dados tratados por meios informáticos, cada vez representam mais a larga maioria das operações e dos meios de tratamento utilizados hodiernamente nas empresas.

Este é, indubitavelmente, um dos artigos que a nova lei de protecção de dados portuguesa, que revogará a Lei 67/98, deveria especificar com mais detalhe todos os certos critérios algo ambíguos no texto do RGPD.

Refira-se o conceito de adequação e as consequências práticas associadas.

A palavra “adequados” é várias vezes empregue, a cada tipo de operação de tratamento que necessitará de cuidados redobradas, e que em algumas circunstâncias terão mesmo de adoptar-se medidas de segurança de informação como a pseudonimização e a cifragem dos dados pessoais.

É dada uma ampla margem de decisão ao próprio responsável pelo tratamento e ao subcontratante (se for o caso), o que pode originar um enorme leque de critérios para definir e implementar as medidas de segurança do tratamento.

Medidas adequadas ou que dêem jeito, eis a questão.

O artigo começa por dizer que têm que ser tidas em conta as técnicas mais avançadas, sempre com a salvaguarda dos custos de aplicação, as finalidades do tratamento e os riscos associados a esse tratamento que possam pôr em causa os direitos e liberdades dos titulares.

Dito isto, poderá perguntar-se: uma empresa que não tenha capacidade financeira para suportar os custos da adopção de medidas de segurança do tratamento exigidas está livre destes compromissos? Ou uma empresa que simplesmente considere que a probabilidade de ocorrer um incidente de violação de dados pessoais é suficientemente baixa, pode “pacificamente”

decidir que não necessita de tomar qualquer medida a este respeito? Ou ainda: poderá uma empresa argumentar que, feita a avaliação de risco, considerou que a colocação de uma palavra-passe no sistema que gere os dados pessoais nessa organização é a medida técnica ideal e suficiente para garantir a segurança do tratamento?

Todas estas questões poderão ter múltiplas razões a suportar várias respostas, e ainda assim válidas. Dir-se-á que é uma questão de perspectiva e de motivações.

Quem estiver próximo do ambiente informático tenderá a considerar que as medidas técnicas que constam do artigo 32º são de implementação obrigatória e crucial para garantir a segurança no tratamento e a conformidade com o RGPD; por sua vez, quem estiver alheado do mundo da informática terá uma predisposição para considerar excessivas as medidas técnicas que requeiram conhecimentos das tecnologias mais actuais, o que faz com que muitos encarem a cifragem, os testes de intrusão, ou uma análise de vulnerabilidades, pura ficção, ou jogos de espiões do 007.

Actualmente, a realidade diz-nos que, o que muitos consideram ficção, já está hoje na prática a acontecer, o que há bem pouco tempo era apenas possível nas produções fantasistas de Hollywood, nos dias que correm com as inúmeras possibilidades tecnológicas, tudo é teoricamente realizável no que respeita ao ciberespaço, não há limitações, há apenas motivações.

Se o que se pretende alcançar informaticamente for rentável, o suficiente ao nível monetário ou outra espécie de motivação, não há impossíveis na persecução de objectivos. Se uma pen com informação encriptada for perdida, e o conteúdo dessa informação for valiosa para uma entidade

privada ou estatal, e que justifique todos os esforços para aceder ao conteúdo dessa informação, demorando mais ou menos tempo, essa informação é acedida.

Mas também é verdade que nem toda a segurança de informação se faz de alta tecnologia. Com o RGPD muitas foram as empresas de software e similares que se colocaram (comercialmente) na linha da frente, garantido que, contratados os seus serviços e produtos, os requisitos de conformidade do Regulamento estariam preenchidos e o problema resolvido.

Com soluções de software, incluídas firewalls, encriptação da informação, complexos sistemas de acesso a plataformas informáticas, palavras-passe complexas e alteradas frequentemente, transmitem a ideia de que esta protecção é “infalível” e suficiente.

Partilha-se a opinião que a segurança do tratamento não são somente as medidas tecnológicas a resolverem os potenciais perigos no tratamento de dados pessoais, bem como também não se está apenas perante um problema de interpretação jurídica, que se possa resolver com medidas organizativas.

Entende-se que será antes um conjunto ponderado de medidas a tomar pelo responsável pelo tratamento.

O responsável pelo tratamento tem que começar por analisar a sua realidade organizativa. Terá que proceder ao levantamento e diagnóstico das categorias de dados pessoais tratados, das operações de tratamento realizadas com esses dados, as finalidades, o número de pessoas que pode

aceder e realizar operações de tratamento, sejam elas acesso, registo, alteração, apagamento ou destruição, entre outras.

Após o inventário e o mapeamento dos dados e das aplicações de suporte às operações de tratamento, o responsável pelo tratamento está em condições de decidir as medidas técnicas e organizativas que considere adequadas.

Em última análise defende-se que, para garantir a segurança, se deverá encarar a segurança da informação de uma forma holística e sistémica, em que as várias componentes da técnica, tecnologia, pessoas e procedimentos, têm que ser pensados e organizados de forma a constituir um sistema robusto, resiliente, coeso, coerente e consequentemente, seguro.

Uma componente pouco discutida, e normalmente encarada como irrelevante ou desprezível é a componente humana. As pessoas são uma importante peça neste puzzle a resolver.

Dificilmente se consegue garantir um sistema de segurança de informação sem considerarmos o papel das pessoas que diariamente manuseiam os dados, protegem os locais, determinam os acessos, decidem, transportam, partilham, conversam... (Enfim são pessoas)!

Podemos ter um sistema informático actualizadíssimo, potentes firewalls, câmaras de videovigilância, segurança física, acessos por análise biométrica, e, no entanto, temos um funcionário com a palavra-passe escrita no normal post-it no ecrã do computador.

4.2 A distinção entre *Privacy by Design & Privacy by Default*

No atinente a este ponto, começa-se por assinalar a imprecisão na tradução portuguesa da expressão *"by default"* que poderá induzir em erro quem considere à letra a expressão adoptada "por defeito". Em português, o termo "por defeito", pode ter duas leituras diferentes: pode ser assumido como o contrário de por excesso, ou pode significar por pré-definição, por princípio, que é o pretendido neste caso.

Dilucidado este ponto e indo ao encontro do artigo 25º, que nos convoca para encarar a protecção de dados desde a concepção e por defeito, é importante referir que o conceito "desde a concepção" tem duas implicações, a saber: uma é a orientação para definir as regras a implementar quando se desenha um novo sistema de protecção de dados, a outra orientação é para se ajustarem as práticas existentes às necessidades de aplicação de novas medidas técnicas e organizativas, indo ao encontro do artigo supracitado.

E o que se pretende é a persecução de alguns dos princípios fundamentais da protecção de dados, como sejam a minimização dos dados, os tempos de conservação a limitação das finalidades, e outros.

Ao contrário do que seria recomendável, e nos raros casos em que as organizações já tinham precauções com procedimentos de protecção de dados, as respostas eram normalmente dadas no seguimento de incidentes de violação de dados pessoais ou de sansões da autoridade de controlo.

O objectivo dos novos paradigmas é encarar estas medidas de protecção de dados desde a concepcção e por pré-definição, como pressupostos do

desenho do sistema a implementar. Como partes primeiras de um todo maior.

O sentido do artigo, em apreço, é o de relevar uma visão preventiva e não uma visão com recurso a medidas avulso, reactivas ou improvisadas, mas tomadas apenas e só com o intuito de remediar ou adiar um problema.

Quantas organizações têm os acessos às bases de dados pessoais acessíveis a todos os funcionários? Muitas vezes sem qualquer restrição de acesso e de limites às operações de tratamento, podendo qualquer um, registar, alterar, e até extrair dados e levar consigo, para fora do seu ambiente profissional, com todos os riscos inerentes a este tipo de comportamentos.

Assim, urge tomar consciência de que os dados pessoais apenas podem ser tratados para a finalidade para a qual foram recolhidos, até serem apagados ou destruídos assim que cessem as finalidades, considerando ainda a exigência de prazos legais definidos em legislação associada para os fins da actividade.

É preciso garantir que, durante todo o processo de tratamento, apenas acedem aos dados quem tiver necessidade de os tratar, desde a definição dos meios de tratamento e durante as operações realizadas com dados pessoais.

4.3 Avaliação do Risco

Como exposto em pontos anteriores, o Regulamento 2016/679 sugere que as organizações adoptem uma política baseada no pensamento de risco, remetendo para uma visão pró activa e consistente sobre a avaliação dos riscos associados às operações de tratamento de dados.

Para certos tipos e níveis de tratamento de dados, em especial com recurso a novas tecnologias, o RGPD insta os responsáveis pelo tratamento a procederem a uma avaliação prévia dos riscos associados às operações a realizarem.
Na sequência da avaliação criteriosa dos riscos, o responsável deverá tomar as decisões adequadas para a implementação das medidas técnicas e organizativas que se justificarem para a defesa dos direitos, liberdades e garantias dos titulares de dados pessoais. O RGPD, no seu artigo 35.º refere-se, explicitamente, à avaliação de impacto sobre a protecção de dados, também conhecida como DPIA[47].

Os vários artigos correspondentes ao capítulo IV do RGPD, que aludem às obrigações do responsável do tratamento e do subcontratante, referem, em abundância, a necessidade de ter em conta os riscos para os direitos e liberdades das pessoas singulares. Realçam também os cuidados a ter com os riscos decorrentes do tratamento inerentes à probabilidade e à gravidade, variáveis de ocorrer uma violação de dados pessoais.

[47] DPIA (Data Privacy Impact Assessment) - Avaliação de Impacto da Privacidade de Dados é um processo destinado a avaliar a necessidade e a proporcionalidade de um processamento de dados pessoais, com identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos.

Como anteriormente referido, podemos constatar uma presença acentuada do factor risco.

A secção 3 do Capítulo IV encaminha-nos para um importante elemento, que será fundamental, para que o todo o sistema funcione em conformidade, a saber: a avaliação de impacto sobre a protecção de dados, e o consequente pedido de consulta prévia, se nessa avaliação se concluir que determinado tratamento de dados a realizar, comportaria um elevado risco para os titulares de dados. Nestes casos é recomendado consultar a autoridade de controlo, para que esta possa dar orientações no sentido de atenuar o possível risco.

Não há protecção de dados pessoais sem uma identificação das potenciais vulnerabilidades do sistema e uma adequada avaliação dos riscos que pode comportar para o titular dos dados. Assim, considera-se obrigatória uma análise de risco, em cada fase da arquitectura da construção de um sistema de gestão de protecção de dados, para tomar as decisões correctas, quanto aos meios às medidas técnicas e organizativas adequadas a cada situação, evitando-se erros por excesso ou por defeito.

4.4 Norma ISO 27001

Neste ponto, que dedicamos à abordagem normativa da segurança da informação, e de todas as medidas exigidas pelo RGPD aos responsáveis pelo tratamento, vai-se identificando os requisitos e os critérios, que as organizações terão que avaliar e pôr em prática para cumprir com as obrigações impostas.

A Norma ISO 27001 "foi preparada para proporcionar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação"[48], com aptidão para ser um sistema certificado. No seu anexo A, descreve-se um conjunto de pontos de controlo a observar para a segurança da informação.

Esta norma tem sido utilizada para cumprir com as medidas de segurança do tratamento que constam no artigo 32º do RGPD, uma vez que este adopta vários aspectos do controlo da informação referidos na norma.

Pode assim considerar-se que há uma zona de intercepção entre o RGPD e a norma 27001, através da qual é possível, com um elevado grau de sucesso, transpor para as organizações as medidas de segurança de informação requeridas pelo RGPD.

O RGPD mostra uma grande compatibilidade quando colocada lado a lado com as obrigações do RGPD em matéria de segurança da informação. Observa-se uma correspondência considerável, no que diz respeito aos requisitos da norma e às obrigações do RGPD, o que tem levado muitas organizações a equacionar esta via para alcançar a conformidade com o Regulamento, pelo menos no que diz respeito às obrigações de segurança do tratamento, a cumprir pelos responsáveis pelo tratamento e subcontratantes.

Em coerência com a visão holística e sistémica de uma organização, e para um melhor desempenho das medidas de segurança da informação a

[48] Norma NP ISO/IEC 27001: 2013, Instituto português da qualidade, p. 5.

implementar sugere-se que sejam integradas no restante sistema de gestão da protecção de dados, para assegurar a conformidade com o RGPD.

Há uma evidente complementaridade nas medidas técnicas e organizativas requeridas no artigo 32º do RGPD e a Norma ISO 27001.

É importante realçar que uma certificação ISO 27001 apenas atesta o exercício de boas práticas nesta matéria, o que contribui para o objectivo de comprovar a conformidade regulatória em protecção de dados.

Pode ser utilizada como elemento para demonstrar o cumprimento das obrigações estabelecidas no artigo 32º do RGPD, designadamente a confidencialidade, integridade, disponibilidade e resiliência dos sistemas que tratem dados pessoais, e o plano de recuperação e restabelecimento do acesso aos dados pessoais em caso de incidente.

Mas a certificação não isenta de responsabilidades o responsável pelo tratamento.

Outra obrigações do RGPD alinhada com a implementação da ISO 27001, são os pontos de controlo para verificar e avaliar, de forma sistemática e periódica, a eficácia das medidas tomadas no sentido de garantir a segurança do tratamento.

Os requisitos da 27001 podem ser importantes na interpretação de alguns termos presentes no n.º1 do artigo 32º do RGPD, tais como o conceito de “adequação”.

O conceito de adequação, que é repetido três vezes no mesmo parágrafo, não aparece associado a qualquer sugestão de medidas técnicas e organizativas, ainda que em termos mais gerais.

Ainda que fora do âmbito da certificação, entende-se que é de toda a utilidade, os responsáveis pelo tratamento, ou um terceiro que trate dados por conta deste, considerarem e seguirem os requisitos definidos na ISO 27001, como um "road map" já que permitem um amplo espectro de possibilidades para dar resposta às obrigações do Artigo 32.º

A título de exemplo veja-se o seguinte caso de compatibilidade entre a norma e o RGPD. A norma 27001 refere que "O estabelecimento e a implementação de um sistema de gestão de segurança da informação de uma organização são influenciados pelas necessidades e objetivos da organização, pelos requisitos de segurança, pelos processos organizacionais utilizados e pela dimensão e estrutura da organização".

O RGPD no ponto 1 do artigo 32º, referente à segurança do tratamento, enquadra as medidas técnicas e organizativas a implementar nas especificidades da organização, e o seu contexto, num claro exemplo de correlação com a norma.

4.5 Medidas de Segurança de Informação

O RGPD obriga o responsável pelo tratamento e os subcontratantes a aplicar medidas técnicas e organizativas que estes considerem adequadas, para garantirem um elevado nível de protecção nas operações de tratamento que realizam. Para o efeito, existem um conjunto de possibilidades

tecnologicamente avançadas. Mas existem também outras possibilidades de implementação de medidas, bem mais simples, como por exemplo um cadeado com chave num armário. O que poderá ser uma medida adequada e sujeita a controlo.

Cada responsável ou subcontratante tem a liberdade de escolher as medidas que considere mais adequadas à sua realidade e contexto específicos.

Para manter a integridade e a confidencialidade dos dados são sugeridas algumas medidas, como a encriptação, cifragem, ou pseudonimização, com o objectivo de garantir a resiliência, a continuidade, e a disponibilidade dos sistemas que gerem dados pessoais.

4.5.1 A tecnologia Blockchain

O *Blockchain*[49], conhecido pela difusão das criptomoedas[50], tem sido ultimamente encarado como possível solução para garantir a protecção de

[49] *Blockchain* é uma base de dados pública distribuída que mantém um registo permanente das transações digitais. Por outras palavras, é um arquivo de dados que armazena um registo imutável de todas as transações digitais. Esta base de dados distribuída não é controlada por uma instituição central, é por sua vez, uma rede de base de dados replicados (o que significa que cada nó na rede armazena a sua própria cópia da cadeia de blocos) que é compartilhado e visível para qualquer pessoa dentro da rede - Ciobanu, Alexandru – *"Tecnologia Blockchain na Industria de Mercados Financeiros – Caso BNP Paribas Securities Services",* Dissertação de Mestrado em Gestão e Estratégia Industrial - ISEG, 2018, p.4

[50] Moeda digital, meio de troca que utiliza o sistema Blockchain e a criptografia para assegurar a validade das transações e a criação de novas unidades da moeda de forma descentralizada. A mais conhecida é o Bitcoin.

dados pessoais no ciberespaço, respondendo assim a algumas das obrigações exigidas pelo RGPD.

Como o nome indica, o *Blockchain* não é mais do que uma cadeia de blocos onde são registadas "transações" – ou acordos entre partes sem a necessidade de uma entidade central – salvaguardadas com mecanismos de cifra forte, para que qualquer alteração num dos elos da cadeia resulte na perda da integridade de toda a cadeia.

Cada "transacção" é replicada automaticamente em vários nós geograficamente distribuídos em cópias da mesma cadeia. A introdução de uma transação na cadeia é sujeita a um mecanismo de eleição entre os vários nós participantes, que garante a integridade da cadeia".[51]

Não cabendo neste trabalho aprofundar as questões técnicas da Blockchain, é importante referir que este sistema de cadeia de blocos, tendo em cada utilizador um nó desta cadeia, permitirá a utilização segura no tratamento de dados e que pode ser aplicada em vários sectores, a saber: a banca, os registos de dados de saúde (categorias especiais de dados), o voto electrónico, e outras transacções e registos do Estado, potenciando o caminho favorável à *e-governance*[52].

Este potencial é reconhecido actualmente em vários estudos, como por exemplo, um estudo da consultora Deloitte de 2017, no qual refere: "Através

[51] Santos, Lino – O Blockchain e o tratamento de dados pessoais por parte do Estado – Workshop - *Proteção de dados pessoais e outras funções do Estado*, FDUNL 8 de março de 2018, Observatório de Proteção de Dados Pessoais/NOVA Direito.

[52] A governação electrónica, é a aplicação das tecnologias da informação e comunicação (TIC) para a prestação de serviços governamentais, troca de informações, integração de sistemas e outros serviços em várias modalidades possíveis entre: governo-cidadãos (G2C), governo-governo (G2G), governo-negócios (G2B). Neste trabalho coloca-se a tónica no G2C, tratando-se de dados pessoais.

da tecnologia Blockchain, será possível pela primeira vez, que duas partes ou mais, estabeleçam acordos, executem transações e construam valor sem a necessidade de intermediários (bancos, agências, governo), que verifiquem as suas identidades, e executem o modelo de negócios – contratos, liquidação e tarefas de manutenção/gestão de registos." [53]

No que diz respeito à protecção de dados, a utilização do Blockchain apresenta algumas vantagens, como por exemplo, a construção de um sistema de protecção de dados desde a concepção (*by design*), garantindo este princípio (requisito) pelas ferramentas que as várias tecnologias que sustentam o Blockchain permitem.

Também em termos de anonimização, o Blockchain permite uma identidade digital, que será apenas associada a uma identidade real, se o titular assim o consentir e desejar. Garante ainda um controlo de acessos bastante eficiente, que poderá ser muito útil na rastreabilidade das operações de tratamento de dados, devido à principal característica do Blockchain – a imutabilidade da informação e dos acessos.

Apesar de ser uma promissora oportunidade, este sistema tem algumas deficiências no que concerne ao exercício dos direitos dos titulares de dados. O direito à portabilidade, e o direito ao apagamento coloca algumas limitações à utilização do Blockchain no campo da protecção de dados.

Devido ao rápido progresso das inovações tecnológicas, é sempre difícil garantir a migração de informação para novos sistemas ou aplicações, sejam dados pessoais ou outros.

[53]Este estudo foi realizado pela consultora Deloitte em 2017, pode ser consultado em https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf, consultado em 27/12/2017.

Nesta tecnologia, o exercício do direito ao apagamento é difícil de ser garantido, uma vez que num sistema de nós, numa cadeia, que poderá ser composta por milhares ou milhões de utilizadores é impossível, querendo eliminar um dado definitivamente, garantir que todos os intervenientes na cadeia o façam.

Não sendo a resposta ideal para todas as dificuldades de garantia da segurança no tratamento de dados pessoais, é ainda assim, uma possibilidade a considerar para futuro.

4.5.2 Cloud computing

A *cloud com*puting[54] é outro caminho possível que pode ser, num futuro próximo, utilizado para acomodar algumas das necessidades a cumprir com as exigências de leis relacionadas com a protecção de dados.

O armazenamento na "nuvem" sofreu um aumento exponencial nos últimos anos e é considerada uma das formas mais seguras e controladas de armazenar dados.

Várias empresas e organismos públicos utilizam este meio, mas é importante identificar os perigos e avaliar os riscos inerentes à utilização da Cloud computing: *"cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources*

[54] Enisa, (2009), "*Report about Cloud Computing- Benefits, risks and recommendations for information security"*, p.4. disponível em http://www.enisa.europa.eu/ (consultado em março de 2017).

and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective" [55]. Como sobressai da citação anterior há, mais uma vez, algumas questões pouco esclarecidas em matéria de segurança.

Algumas das preocupações prendem-se com a garantia da confidencialidade e da integridade da informação. O facto de muitas vezes não ser conhecido o espaço físico do armazenamento é algo incompatível com alguns critérios básicos da segurança e da protecção de dados.

Esse facto revela-se na dificuldade em obter certificações de segurança quando o fornecedor de *Cloud* não garante tudo o que é necessário, em termos de segurança de informação, como por exemplo a possibilidade de auditar os sistemas de redes informáticas e o espaço físico. O que coloca além de questões técnicas e legais, também questões políticas difíceis de resolver.

Entende-se que os fornecedores de serviços de *Cloud* devem adaptar-se à realidade do RGPD, para poderem operar na União Europeia, e para garantirem e poderem evidenciar o controlo de acessos, a informação de transferências de dados, os processos de notificação de incidentes e as medidas já referidas de segurança do tratamento.[56]

Não pode terminar-se este capítulo sem referir que a segurança da informação tem várias vertentes, e todas elas merecem uma atenção específica. De nada valerá ter um sistema actualizadíssimo, potentes firewalls, hardware topo de gama, se as outras componentes da segurança

[55] *Idem*

[56] Artigo 32º do RGPD

da informação falharem, ou sejam, os recursos humanos que operam com o tratamento dos dados.

"As redes de comunicação são indispensáveis ao funcionamento de praticamente todas as estruturas da sociedade. No nosso dia a dia, é quase certa a utilização de, pelo menos, um serviço dependente de uma rede de comunicação."[57]

As redes são outro factor da segurança da informação a não esquecer. Todos os sistemas que mantenham algum tipo de interoperabilidade têm de garantir a segurança de forma integrada e sistémica, podendo colocar em risco todo o sistema se um elo desta rede não apresentar o mesmo nível de protecção.

[57] Véstias, Mario, *Redes Cisco para profissionais*, FCA - Editora de Informática, Lda, Lisboa, 7ª edição, 2016, p.1

5. O papel do encarregado da protecção de dados na governança das organizações

O Encarregado de Protecção de Dados (EPD) é uma figura juridicamente nova, que o regulamento considera necessária, em certas condições, para a protecção de dados, definindo o seu enquadramento organizativo.

Também esta figura, as suas qualidades, atribuições e exercício das funções, aparece envolta em alguns equívocos e imprecisões.

Mas se é uma figura nova no RGPD, já o mesmo não pode dizer-se sobre o conceito de haver um responsável pela protecção de dados, uma figura que nas organizações garanta o cumprimento das normas da protecção de dados.

Em alguns Estados-Membros, há alguns anos que existe essa figura nas organizações. Poderá mesmo dizer-se que o regulamento assumiu e tentou sistematizar as experiências havidas nos Estados-Membros, com um grau de maturidade superior à média dos restantes estados da União.

O enquadramento do EPD, é definido nos artigos 37º, 38º e 39º do RGPD, que especificam as condições e os requisitos a observar na designação, nos deveres e nas obrigações, nas qualidades profissionais e também as garantias que lhe permitam desempenhar as suas funções.

A figura do EPD será seguramente um dos instrumentos essenciais para que as medidas de protecção de dados sejam implementadas e mantidas com sucesso nas empresas e nos organismos públicos.

O facto de nas organizações, cujo tratamento de dados comporte um maior risco para os titulares, ser obrigatória a designação de um EPD, permitirá que, pelo menos uma pessoa dentro da organização tenha a obrigação de cuidar das práticas da protecção de dados e de assegurar a conformidade. Decorrente das suas responsabilidades e atribuições, o EPD cumprirá e fará cumprir o que for definido pelo responsável pelo tratamento quanto à política de protecção de dados.

O RGPD define quatro situações em que é incontornável e a designação de um EPD, a saber:
- Quando sejam tratados dados pessoais por um organismo público[58];
- Quando o tratamento obrigue a um controlo de dados, regular e sistemático, em grande escala[59];
- Quando sejam tratados dados pertencentes às categorias especiais de dados[60];
- Quando sejam tratados dados pessoais relacionados com condenações penais e infrações[61].

Estas são as situações definidas pelo legislador europeu, para obrigar um responsável pelo tratamento a designar um EPD, deixando aos Estados-Membros a possibilidade de, no seu ordenamento jurídico interno, definir outros critérios cumulativamente com os anteriormente referidos.

[58] Artigo 37.º do RGPD
[59] Ver considerando (91) do RGPD
[60] Artigo 9.º do RGPD - dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
[61] Artigo 10.º do RGPD

No entanto, há situações em que não sendo obrigatório, pode (ainda assim) ser bastante útil designar alguém que responda directamente aos desafios que o RGPD vem colocar.

Entende-se como pertinente o entendimento do Grupo de Trabalho do Artigo 29º (GT 29), que refere o seguinte: "Mesmo quando o RGPD não exige especificamente a nomeação de um EPD, as organizações poderão, nalguns casos, considerar conveniente designar um EPD a título voluntario." [62]

As exigências impostas pelo RGPD, vai implicar nas empresas que tratem dados pessoais, um esforço organizativo, no sentido de garantir a conformidade com as leis da protecção de dados, esforço este deverá estar concentrado numa pessoa, que dirija e responda pelas boas práticas e pela conformidade exigida. Que seja o ponto de contacto com os titulares dos dados, o ouvinte, o sensibilizador e o pedagogo que será necessário para diminuir a potencial conflitualidade. Que seja um interlocutor disponível e competente, junto da Autoridade de Controlo.

Pode dizer-se que é espectável que as empresas venham a precisar de um responsável que responda pela política e pelas práticas da organização sobre a protecção de dados, com controlo sobre sistema, mas simultaneamente um aconselhador, um auditor, um defensor, um diplomata.

[62] Grupo do Artigo 29.º, "Orientações sobre os encarregados da protecção de dados (EPD)", WP 243 rev.01, Bruxelas, 13 de dezembro de 2016, p.7

Quando o responsável pelo tratamento designa um EPD, por obrigação ou por decisão estratégica e voluntária, pode optar por designar alguém interno à organização, ou externo, em regime de prestação de serviços.

Esta decisão fica ao critério do responsável pelo tratamento. Caso a opção recaia sobre um colaborador interno, que deverá ser observada a boa regra de evitar situações que potencializem eventuais conflitos de interesse.

Eventuais conflitos de interesse invalidam a designação de um colaborador interno para esta função. A regra a considerar é que não deve exercer este cargo quem possa determinar as finalidades e os meios de tratamento de dados pessoais[63].

Não é aceitável, do ponto de vista da isenção e da seriedade da função, que um responsável que defina os procedimentos para a realização de operações de tratamento de dados pessoais numa organização, possa posteriormente avaliar e auditar em causa própria, se esses procedimentos cumprem com os requisitos aplicáveis do RGPD.

Um tema pouco consensual, que tem gerado alguma incerteza e até alguma desinformação, é o referente às qualidades profissionais e requisitos obrigatórios para desempenhar esta função[64].

O regulamento é de facto pouco preciso neste capítulo, deixando ao critério da sensatez a avaliação e a escolha das características a possuir para o desempenho das funções de EPD.

[63] Grupo do Artigo 29.º, "Orientações sobre os encarregados da protecção de dados (EPD)", WP 243 rev.01, Bruxelas, 13 de dezembro de 2016, p.19.

[64] Ver Artigo 37º n.º5 e considerando (97) do RGPD.

O RGPD refere que quem for designado como EPD, tem de ter conhecimentos especializados no domínio do direito e domínio das práticas da protecção de dados, pelo que se pressupõe que seja alguém que conhece, em profundidade, o RGPD, bem como as leis internas do(dos) Estado(s)-Membro(s) em que opera o responsável pelo tratamento.

Deve ainda ser capaz de desempenhar as funções de informar, sensibilizar e aconselhar o responsável pelo tratamento, e os trabalhadores intervenientes na realização de operações de tratamento de dados pessoais, bem como informar os titulares dos dados dos seus direitos e obrigações.

Terá também a seu cargo a responsabilidade de formar internamente os quadros técnicos e operacionais que realizem operações de tratamento de dados, e auditar, monitorizar e garantir a conformidade com o RGPD dos procedimentos implementados no domínio da protecção de dados.

5.1 Funções e responsabilidades

O EPD coopera com as autoridades de controlo, enquanto ponto de contacto preferencial sobre a protecção de dados. Tem ainda que ter a capacidade de avaliar, a cada momento, o impacto do tratamento de dados pessoais da organização, para o normal exercício dos direitos e liberdades dos titulares, dos trabalhadores da organização e, simultaneamente, os interesses do responsável pelo tratamento, em consonância com as regras do regulamento.

Estas funções de EPD são, sem dúvida, susceptíveis de criar algumas situações de tensões conflituantes. A este propósito, veja-se o quadro geral das suas atribuições.

O EPD é o garante do cumprimento do RGPD na organização. É o responsável por garantir que os direitos dos titulares estão assegurados para serem exercidos. É quem, internamente, tem a responsabilidade de sensibilizar os trabalhadores e zelar pela protecção dos seus dados pessoais. Como se viu anteriormente, é quem aconselha e informa a gestão de topo da organização sobre as práticas a seguir no tratamento dos dados, de acordo com os requisitos do RGPD.

Como facilmente pode constatar-se, não será tarefa fácil defender simultaneamente os direitos dos titulares dos dados, dos trabalhadores, dos clientes/utentes, e os interesses da organização em conformidade com o RGPD, sem deixar de cooperar com a autoridade de controlo.

O EPD terá de saber gerir com equilíbrio e parcimónia, mas de forma assertiva e firme as decisões que a gestão corrente e os conflitos que surjam, de forma resiliente, mas focada na conformidade com o RGPD. Terá de agir de forma autónoma e independente, sem aceitar ingerências nas suas decisões sobre a protecção de dados.

O legislador europeu, antecipando o quadro complexo e conflitual do exercício de EPD, revestiu a função do EPD de garantias pouco comuns em outras funções de responsabilidade.

O EPD tem que ser envolvido em todos os assuntos que digam respeito à protecção de dados, sendo-lhe disponibilizados todos os recursos

necessários, incluindo a formação para o bom desempenho das suas funções. Tem que ter livre acesso a todos os dados pessoais na organização, bem como às operações de tratamento realizadas com esses dados. Responde directamente à gestão de topo, não recebe instruções relativamente ao exercício das suas funções, e não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções.

Ou seja, no que respeita às decisões do EPD, ninguém dentro da organização pode alterá-las ou contestá-las. O responsável pelo tratamento pode não acolher a opinião ou os pareceres do EPD, tendo neste caso que declarar por escrito, os motivos desta decisão.

Prevendo as consequências derivadas destes casos, o legislador europeu conferiu ao EPD prerrogativas novas e adequadas ao exercício das suas funções.

Para além das qualidades profissionais apontadas pelo RGPD[65], entende-se que o EPD deve ter outras características para um melhor exercício das suas funções com rigor e com eficiência.

Será recomendável a quem assuma esta função, que seja uma pessoa com propensão para ouvir e para dialogar, que mantenha com os seus interlocutores uma relação positiva e construtiva. Grande parte do seu trabalho requer uma avaliação da conformidade legal e do nível de risco, o que exige bom senso e um apurado sentido do dever para chegar à decisão acertada.

[65] Artigos 37.º, e n.º5 do RGPD.

Estas características são ainda fundamentais em alguém que tem que estar preparado ao mesmo tempo para dialogar, informar, aconselhar e até negociar com a gestão de topo, com os titulares de dados pessoais e com os trabalhadores da própria organização.

5.2 Responsabilidade proactiva

Sendo a função do Encarregado de Protecção de Dados recente e inovadora, pelo menos no referente à nossa realidade[66], vão surgindo muitas dúvidas sobre o perfil a considerar na sua designação dentro de uma organização.

Ainda não se dispõe de experiência no comportamento organizativo espectável, nos critérios para medir as capacidades e identificar os atributos que alguém tenha que ter para desempenhar a função.
Ao contrário do que é anunciado em alguns cursos que "certificam" Encarregados de Protecção de Dados em "formações" de dezasseis horas, não existem até à data quaisquer critérios definidos pela autoridade de controlo, ou qualquer entidade certificadora habilitada para tal.

Face ao vazio existente, em que navegam muitas soluções sem solução, era conveniente que a autoridade de controlo apresentasse os critérios a observar para a certificação da função juridicamente estabelecida no RGPD, ajudando a regular um mercado "emergente" onde prolifera muita falta de seriedade e torna-se, cada vez mais, propício às inúmeras faltas de ética.

No mesmo sentido sugere-se que a Autoridade de Controlo defina os critérios para o exercício do cargo de EPD, para avaliar os sistemas de implementação do RGPD nas organizações, eventualmente desenvolvendo

[66] A figura de EPD existe há já bastante tempo em países como a Alemanha ou Suécia.

os caminhos para a certificação, para as marcas e os selos de conformidade, como previsto pelo RGPD[67].

Mesmo sabendo-se que qualquer decisão de certificação é voluntária, e que requer alguma maturidade das organizações, admite-se que pudesse ser bastante útil, numa primeira fase, com muita incerteza sobre o que fazer, muita cosmética e desinformação generalizada sobre o RGPD.

Pelos sintomas do mercado e pela desproporção entre as organizações que precisam de apoio, mas não estão capacitadas para uma postura crítica e activa e todo o tipo de oportunismos, de organizações impreparadas e pouco sérias, que vendem o que querem, ganharia especial relevância uma voz activa por parte da autoridade de controlo.

Em 2017, a Agencia Española de Protección de Datos (AEPD), definiu os critérios para a certificação[68] do *Delegado de Protección de Datos,* permitindo que as entidades certificadoras pudessem ministrar cursos e certificar essa figura.

A congénere espanhola da CNPD deu assim o mote para a certificação de profissionais que queiram exercer esta função, ajudando a balizar os padrões admissíveis para garantir um bom desempenho de um EPD.

As exigências que se colocam a um EPD, pelas suas funções e responsabilidades, enquadrado nas exigências do RGPD, são complexas e variadas. Vão da necessidade de avaliar o risco e o impacto de operações

[67] Artigo 42º do RGPD.
[68]Este documento da agência espanhola de protecção de dados pode ser consultado em: http://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf (consultado em janeiro de 2018)

de tratamento, conhecer e auditar os sistemas que gerem dados pessoais, até conduzir processos de melhoria e de controlo contínuo de todo o tratamento de dados.

O termo *accountability,* muito utilizado na esfera anglo-saxónica, encaixa perfeitamente no que deve ser o comportamento de um EPD. É alguém que desempenha as suas funções com um apurado sentido da responsabilidade, com ética e com brio, salvaguardando, quer os interesses da organização que representa quer os titulares dos dados, em consonância com a autoridade de controlo, com todo o rigor, transparência, idoneidade e lealdade. Estes atributos são fulcrais para o sucesso de uma *governance* sustentada da protecção de dados dentro de uma organização.

5.3 Notificação e comunicação de uma violação de dados pessoais

Em caso de violação de dados pessoais, o responsável pelo tratamento, notifica a autoridade de controlo, de preferência no prazo de 72 horas e, caso não o consiga fazer, terá que justificar o motivo da demora[69].

No caso da violação de dados pessoais implicar um elevado risco para os titulares, estes devem ser informados do incidente. O mesmo acontece relativamente à autoridade de controlo. Não podem existir dúvidas sobre a exigência de transparência e de lealdade no tratamento de dados pessoais exigidos pelo RGPD.

Esta é uma obrigação que causa algum desconforto às organizações envolvidas devido ao nível de exposição a que esta questão pode levar. A

[69] Artigo 33º do RGPD.

experiência diz que, quando ocorre um incidente de violação de dados pessoais, o mais comum é manter o sigilo e a reserva quanto ao sucedido. Principalmente se a violação em questão não for conhecida por terceiros, nem pelos titulares afectados.

Diariamente existem casos destes, por exemplo na actividade bancária, onde ocorrem inúmeros incidentes de violação de dados pessoais dos titulares através das aplicações de *homebanking*[70]*.* Apesar da imagem que se transmite ao cliente, de que o sistema é inviolável e completamente seguro, a realidade é, em muitos casos, bem diferente.

Este é um dos casos típicos em que a comunicação pública de um incidente de violação de dados pessoais pode traduzir-se num enorme impacto negativo para a reputação de um banco. Será que continuarão nestes casos a proceder da mesma forma, escondendo os incidentes?

A tendência parece ser para a continuidade destas más práticas, pelo menos enquanto não houver mais consciencialização dos titulares e um olhar mais crítico da opinião pública.

Mas não pode esquecer-se o papel altamente dissuasor das sanções, que ajudam a relevar o papel preventivo do EPD. As sanções, neste novo quadro jurídico, poderão atingir 20 milhões de euros ou, no caso das empresas, poderão ser 4% do volume de negócios mundial por ano.
Ainda sobre o quadro sancionatório, e para além da densificação espectável da legislação nacional, convém não esquecer que existe ainda a

[70] O Homebanking é o simples acto de realizar operações bancárias através da Internet, sem ter de se deslocar até um Banco ou qualquer caixa multibanco. Pode consultar-se variada informação financeira e pessoal, fazer transferências ou pagamentos através dos bancos online com a toda a conveniência.

possibilidade de uma organização ver negado o direito ao tratamento de dados, cujo impacto será desastroso para o negócio.

Também no caso de notificações de incidentes, o EPD terá um papel relevante, ao contribuir para uma análise das condições de uma hipotética ou real ocorrência de uma violação de dados pessoais. A existir, o EPD tem que avaliar o nível de risco para os direitos e liberdades das pessoas singulares, tomar decisões sobre as informações a prestar e as medidas a empreender para minimizar os possíveis danos para os titulares.

5.4 Consulta prévia

Havendo um EPD[71] designado, deverá ser-lhe solicitado um parecer sobre a avaliação de impacto e de risco das operações de tratamento de dados efectuada pelo responsável pelo tratamento.

Se o EPD considerar que o tratamento a efectuar é susceptível de implicar um elevado risco para os titulares, o responsável pelo tratamento, com a recomendação do EPD, poderá solicitar uma consulta prévia à autoridade de controlo, solicitando uma avaliação às medidas previstas implementar pela organização.
Assim pode salvaguardar eventuais sanções por adopção de medidas desadequadas ou mesmo que por violarem o disposto no regulamento.

Para a consulta prévia podem contribuir operações de tratamento que impliquem um tratamento automatizado, definição de perfis, ou dados pertencentes às categorias especiais e com informação sobre condenações e infracções, vulgo registo criminal.

[71] Artigo 35º n.º2 do RGPD

6. Conclusões

O RGPD constitui uma peça jurídica fundamental para a uniformização das ordens jurídicas dos Estados-Membros da União, quanto à protecção no tratamento dos dados das pessoas singulares e à sua livre circulação;

Como regulamento é de aplicação obrigatória em todos os Estados-Membros, sobrepondo-se às ordens jurídicas nacionais, de modo a por fim à dispersão jurídica existente;

Os aspectos menos precisos, a incorporação de alguns conceitos mais vagos, alguma complexidade na exposição dos artigos e vários tipos de remissões, entre outros aspectos menos positivos, não desqualificam nem diminuem o RGPD como um marco na defesa dos direitos, liberdades e garantias dos titulares dos dados;

A legislação de cada Estado-Membro sobre a protecção de dados, em complemento ao regulamento, o papel da respectiva autoridade de controlo e as diversas experiências das organizações na abordagem ao RGPD, no sentido da conformidade e da responsabilidade demonstrável, irão permitir ganhos de maturidade e de assertividade, com a identificação dos aspectos a melhorar para uma revisão do documento de modo a torna-lo mais claro e preciso;

As autoridades de controlo de cada Estado-Membro têm um papel e uma responsabilidade fundamentais na credibilização do RGPD e de uma política de protecção de dados, devendo solicitar todos os meios que forem considerados necessários para uma razoável intervenção pública, seja num pendor mais pedagógico ou mais sancionatório;

Desde Maio de 2016 que os organismos públicos, as associações sectoriais e as empresas privadas desaproveitaram os dois anos de vacatio legis, numa perda de tempo generalizada para conhecer o regulamento, identificar o impacto nas organizações, avaliar os recursos humanos, técnicos e financeiros a afectar ao processo de implementação e de manutenção de um sistema de protecção de dados;

Às portas da entrada em aplicação do RGPD, assiste-se a um despertar tardio e preocupado das organizações, em especial pelo espectro sancionatório. Salvo algumas excepções, o mercado está a agitar-se de forma algo apressada, na procura de soluções rápidas, quase pré-fabricadas, que permitam uma "importação documental" de aplicação expedita;

A insensibilidade de muitas organizações, que as impede de ver as oportunidades que o RGPD pode impulsionar, deixa-as com uma visão passadista e desconfortável, avessa à mudança. A gestão da mudança é a chave para a implementação e a manutenção de uma política e de práticas organizativas de protecção de dados em conformidade com o regulamento;

A mudança do paradigma regulatório, numa nova perspectiva de responsabilidade pró-activa e auto-regulatória vai levar o seu tempo, não só para os responsáveis pelo tratamento como para os subcontratantes, e outros actores deste cenário do novo quadro jurídico da protecção de dados.

A figura do Encarregado de Protecção de Dados é uma pedra basilar do regulamento. O legislador antecipou que sem esse "ponto" de apoio, a

implementação e, em especial, a manutenção de uma política e práticas organizativas para a protecção de dados, em conformidade demonstrável com o RGPD estariam comprometidas;

As organizações que designem um Encarregado de Protecção de Dados, por obrigação regulatória ou por decisão voluntária, ficarão em melhores e mais robustas condições para um desempenho controlado e consistente da política de protecção de dados, num quadro de conformidade;

Nesse pressuposto, as organizações têm que assegurar ao Encarregado de Protecção de Dados os recursos e as condições adequados, para um desempenho cabal das suas atribuições, no respeito pelo seu perfil e papel no diálogo com os titulares dos dados e a autoridade de controlo;

Por fim, uma conclusão sobre esse mundo novo, que é o ciberespaço. Num contexto repleto de rápidos avanços tecnológicos, que permitem cada vez mais transferências de dados pessoais, e cada vez menos controlo da nossa informação pessoal, no qual acrescem os riscos e os desafios de elevado grau, entende-se que este é um espaço que merece um olhar mais crítico, numa perspectiva de encontrar as melhores formas para tentar controlá-lo e regulá-lo.

7. Bibliografia

- ANDRADE, Priscila (2013). "Quem vigia o vigilante? entre a vigilância e a privacidade na sociedade em rede". Dissertação de mestrado em Comunicação, Cultura e Tecnologias da Informação, no ramo Internet e Comunicação em Rede, Departamento de Sociologia, ISCTE Instituto Universitário de Lisboa.

- BEAL, Adriana, *Gestão Estratégica da Informação*, Atlas, Brasília, 2008, p.19.

- BECK, Ulrich, *Sociedade de Risco Mundial, em busca da segurança perdida*, Edições 70, Lisboa, 2015, pp. 103 a 108.

- CASTELLS, Manuel, A Galáxia Internet, Edição – Fundação Calouste Gulbenkian, 2ª Edição, 2007.

- CASTRO, Catarina Sarmento, Direito da Informática, Privacidade e Dados Pessoais, Almedina, 2005.

- CIOBANU, Alexandru (2018). "Tecnologia Blockchain na Industria de Mercados Financeiros – Caso BNP Paribas Securities Services". Dissertação de Mestrado em Gestão e Estratégia Industrial – ISEG, p.24.

- DIAS, Cátia Alexandra Horta (2013). "A videovigilância e o direito à privacidade do trabalhador", Dissertação de mestrado em Direito das Empresas, Departamento de Economia Política, ISCTE Instituto Universitário de Lisboa, p.32.

- DRUCKER, Peter, Desafios da gestão para o século XXI, Livraria Civilização Editora, 2000, pp.114 a 116.

- DUARTE, Ana Teresa Veiga (1998). "A privacidade e a sociedade informatizada, ". Dissertação de mestrado em Comunicação, Cultura e Tecnologias da Informação, Departamento de Sociologia, Instituto Superior de Ciências do Trabalho e da Empresa – ISCTE, p.11.

- FARINHO, Domingos Soares, Intimidade da Vida Privada e Media no Ciberespaço, Almedina, 2006.

- FERNANDES, José Pedro Teixeira, Ciberguerra, Quando a utopia se transforma em realidade, Verso da História, 1ª edição, Vila do Conde, 2014.

-FONTAINHAS, Emília da Conceição Golim (2013). "Dos Testemunhos de Conexão no Quadro Legislativo Europeu da Proteção de Dados, em particular do

consentimento para a sua utilização". Dissertação de Mestrado Mestrado em Direito e Informática, Universidade do Minho, pp. 19 a 22.

- GIBSON**,** William**,** Neuromancer (eBook)**,** Aleph, 2015.

- GOUVEIA, Jorge Bacelar, et al, Leis de Direito da Segurança, 2a edição, Quid Júris, 2014.

- GUERRA, Amadeu, A Lei da Proteção de Dados Pessoais, em "Direito da Sociedade da Informação", Volume II, Coimbra Editora, fevereiro de 2001.

- LEONHARD, Gerd, Tecnologia versus Humanidade, Editora Gradiva, 2017.

- LÉVY, Pierre, *Cibercultura, Epistomologia e sociedade*, Instituto Piaget, Lisboa, 2000. p. 16.

- PAYTON, Theresa M. ; CLAYPOOLE, Theodore, co-aut. - Privacy in the age of big data : recognizing threats, defending your rights, and protecting your family. Rowman & Littlefield, 2014.

- PEREIRA, Ricardo Manuel Amaro (2015). "Proteção da Privacidade em Sistemas de Dados". Dissertação de Mestrado em Engenharia Informática - Universidade do Minho.

- PEREIRA, Rui - Estudos de Direito e Segurança, Volume II, coordenação Jorge Bacelar Gouveia, Almedina, 2015.

- PINHEIRO, Alexandre Sousa - Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional, Lisboa, AAFDL, 2015, p.118.

- PINTO, João Miguel Jardim de Abreu Ferreira (2015). "Direito ao Esquecimento Digital 2.0: Motores de busca da Internet após o Acórdão Google Spain (C-131/12)". Dissertação de Mestrado em Segurança da Informação e Direito do Ciberespaço -FDUL.

- RODOTÀ, Stefano, *El derecho a tener derechos*, trotta, Madrid, 2014, p.84.

- SANTOS, José Lino Alves dos (2011). "Contributos para uma melhor governação da cibersegurança em Portugal". Dissertação de Mestrado em Direito e Segurança, FDUNL.

- SCHMIDT, Eric & COHEN, Jared – *A Nova Era Digital – Reformulando o futuro das pessoas, das nações e da economia*, D.Quixote, 2013, Lisboa, p. 185.

- SOUSA & MIGUEL, Segurança no Software, FCA – Editora de Informática, Lisboa, 2010.

- SOLOVE, Daniel J.. The digital person: technology and privacy in the information age. New York: New York University Press, 2004.

- SILVA, Heraclides Sequeira dos Santos (2018). “A Protecção de Dados Pessoais na Era Global: O Caso Scherems”. Dissertação de Mestrado em Direito – FDUNL.
- TOFFLER, Alvin, *A Terceira vaga*, 1.ª edição, vida e cultura, Lisboa, 1984.

- VÉSTIAS, Mario, *Redes Cisco para profissionais*, FCA - Editora de Informática, Lda, Lisboa, 7ª edição, 2016, p.1.

- VERDELHO, P., R. Bravo, & M. L. Rocha. As Leis do Cibercrime, Vol. I. Lisboa: Edições Centro Atlântico, 2003.