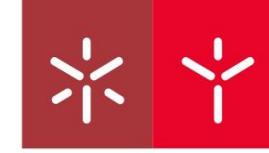




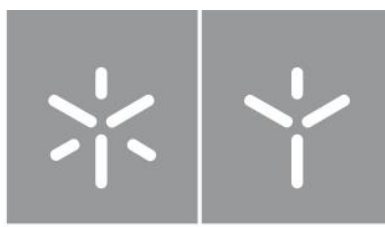
Beatriz Brandão de Sousa

A proteção de dados pessoais e o quadro
regulatório atual – pistas de reflexão para
uma heterorregulação mitigada?

Universidade do Minho
Escola de Direito







Universidade do Minho
Escola de Direito

Beatriz Brandão de Sousa

A proteção de dados pessoais e o quadro
regulatório atual – pistas de reflexão para
uma heterorregulação mitigada?

Dissertação de Mestrado
Mestrado em Direito Administrativo - com
especialização em Direito Administrativo Especial

Trabalho efetuado sob a orientação da
Professora Doutora Joana Covelo de Abreu

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença [abaixo](#) indicada.

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

Licença concedida aos utilizadores deste trabalho



**Atribuição
CC BY**

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

Agradecimentos

Dedico esta dissertação à minha família e amigos. Pela paciência, amor e carinho neste caminho. Um obrigado nunca será suficiente para vocês.

Dedico ainda à minha orientadora por me ter ajudado a navegar pelas dificuldades sempre com os melhores conselhos e recomendações quer quanto à sugestão do tema quer quanto ao melhor caminho em termos de investigação científica.

A vocês,

Obrigada mais uma vez.

DECLARAÇÃO DE INTEGRIDADE

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

Mais

A proteção de dados pessoais e o quadro regulatório atual – pistas de reflexão para uma heterorregulação mitigada?

Resumo

A presente dissertação trata de um tema atual que se encontra em permanente evolução e adaptação às expectativas e necessidades que a sociedade vai apresentando. O impacto das novas tecnologias de informação e de comunicação é evidente na vida em sociedade, determinando que os dados pessoais conheçam hoje um quadro regulatório mais ambicioso. No entanto, cabe equacionar se a solução encerrada na legislação aplicável – que parece surgir como uma heterorregulação, pois pressupõe a intervenção de uma autoridade reguladora nacional (a autoridade de controlo), mas mitigada, na medida em que confia nas diligências levadas a efeito pelos responsáveis pelo tratamento – é suficiente para os avanços tecnológicos verificados.

Palavras-chave: dados pessoais, RGPD, Administração Pública, responsável pelo tratamento.

The protection of personal data and the current regulatory framework – clues for reflection for mitigated heteroregulation?

Abstract

This dissertation deals with a current topic that is constantly evolving and adapting to the expectations and needs that society is presenting. The impact of new information and communication technologies is evident in life in society, which means that personal data now has a more ambitious regulatory framework. However, it is important to consider whether the solution set out in the applicable legislation - which appears to be heteroregulation, as it presupposes the intervention of a national regulatory authority (the supervisory authority), but is mitigated insofar as it relies on the steps taken by those responsible for processing - is sufficient for the technological advances that have taken place.

Keywords: personal data, GDPR, Public Administration, data controller.

Índice

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

.....iv

Agradecimentos.....v

DECLARAÇÃO DE INTEGRIDADEvi

Resumovii

Abstractviii

Abreviaturas e Siglasxii

Introdução 1

1. A digitalização..... 3

1.1. A digitalização e a sua evolução..... 4

1.2. Digitalização e a Administração Pública 6

1.2.1. A digitalização da Administração Pública na União Europeia 9

1.2.2. Programas a nível nacional 11

1.3. Principais problemáticas da digitalização 14

1.3.1. Problema da proteção de dados..... 15

2. Proteção de dados 17

2.1. Conceito de dados pessoais 20

2.1.1. Informações relevantes..... 22

2.1.2. Relativa a 24

2.1.3. Pessoa identificada ou identificável 25

2.1.4. Pessoas singulares 26

2.1.5. Casos problemáticos 28

2.2. Tratamento dos Dados Pessoais 30

2.2.1. Consentimento 32

2.2.2. Princípios aplicáveis em matéria de proteção de dados 34

2.2.2.1. Princípio da Lealdade..... 36

2.2.2.2. Princípio da Segurança	39
2.2.3. Problemáticas do tratamento de dados pessoais	41
3. Violações de Dados.....	42
3.1. Procedimento em caso de violação de dados.....	43
3.2. Entidades competentes na responsabilidade	46
3.2.1. Entidades competentes a nível da União Europeia	47
3.2.2. Entidades competentes a nível nacional	49
3.2.2.1. Comissão Nacional de Proteção de Dados.....	54
3.2.2.1.1. Funções das autoridades de controlo	57
3.2.2.1.2. Poderes de investigação	57
3.2.2.1.3. Poderes de correção.....	58
3.2.2.1.4. Poderes consultivos e de autorização.....	59
3.2.2.2. Encarregado de proteção de dados	59
3.2.2.3. Responsável pelo tratamento	61
3.2.2.3.1. Conceito e critérios determinantes do que se entende por responsável pelo tratamento.....	63
3.2.2.3.2. O responsável tem de ser uma pessoa singular ou coletiva, sendo esta uma autoridade pública, uma agência ou outro organismo.....	64
3.2.2.3.3. Responsável de forma individual ou em conjunto com outro responsável.....	65
3.2.2.3.4. Que define as finalidades do seu tratamento de dados e os meios para as concretizar.....	67
3.2.2.3.5. Competências assumidas pelo responsável pelo tratamento.....	70
3.2.2.3.5.1. Definição das finalidades	70
3.2.2.3.5.2. Meios de tratamento	71
3.2.2.3.6. Obrigações do responsável pelo tratamento de acordo com as suas competências.....	72

3.3. Responsabilização em caso de violação de dados	75
3.3.1. Principais modificações legislativas entre 1995 e 2018 – o impacto na perceção da regulação de heterorregulação a heterorregulação mitigada?.....	76
3.3.1.1. Diretiva 95/46/CE.....	77
3.3.1.2. Regulamento (UE) n.º 679/2016, de 27 de Abril.....	81
3.3.1.3. Heterorregulação mitigada	84
Conclusão	90
Lista Bibliográfica	92
Bibliografia Eletrónica	94
Legislação, Diretrizes e Pareceres	95
Jurisprudência	97

Abreviaturas e Siglas

AEPD – Autoridade Europeia para a Proteção de Dados

AIPD - Avaliação de Impacto do Tratamento de Dados

AMA – Agência para a Modernização Administrativa

AP – Administração Pública

CC – Código Civil

CE – Comissão Europeia

CNPD – Comissão Nacional de Proteção de Dados

coord. – Coordenação

CTIC – Comunicação na Administração Pública

dir. - Diretor

ed. – Editor

eds. – Editores

IDES – Índice de Digitalidade da Economia e da Sociedade

n.º - Número

ORECE - Organismo de Reguladores Europeus das Comunicações Eletrónicas

RAT – Registo de Atividades de Tratamento

RGPD – Regulamento Geral sobre a Proteção de Dados

TFUE - Tratado sobre o Funcionamento da União Europeia

UE – União Europeia

Introdução

A digitalização da sociedade tem ocorrido um pouco por todo o mundo, modificando o modo como as atividades sociais, económicas e políticas são praticadas, em resultado da permanente evolução que a vida em sociedade vai exigindo e a capacidade de investimento vai possibilitando que assim ocorra. Esta evolução passa, em parte, pelo recurso à tecnologia como forma de resposta que permite uma maior fluidez na prática de atos necessários para a vida em sociedade ou para a satisfação dos interesses dos cidadãos. A percepção de que o desenvolvimento impõe, em parte, o reconhecimento das vantagens da tecnologia foi um dos primeiros passos essenciais para que a digitalização ocorresse e tivesse o impacto que tem na sociedade. O conhecimento das modificações positivas que poderiam ocorrer e de que modo poderiam os cidadãos e os Estados beneficiar foi a motivação para o investimento feito numa fase inicial em que apenas se conhecia o que era espectável e ainda não havia resultados concretos da aplicabilidade a grande escala das tecnologias. Com o investimento dos governos e a criação de meios tecnológicos com capacidade de atuar como influenciadores e modificadores da vida em sociedade, tornou-se possível que se começasse a perspetivar outros modos de se praticarem atos, de se recorrer a um determinado serviço ou concretizar determinado interesse por parte do cidadão ou do Estado. Os primeiros passos foram, sem dúvida, desafiantes a todos os níveis e impuseram uma coordenação de diferentes e diversos meios e conhecimentos para que a utilização dos benefícios da tecnologia pudesse ser feita da melhor forma.

As Administrações Públicas assumiram um papel de destaque como representantes dos seus cidadãos e como uma das principais interessadas em que os benefícios da tecnologia fossem aplicáveis aos serviços públicos. Há uma exigência e necessidade de que a sua atuação seja sempre aquela que melhor representa e corresponde aos interesses dos cidadãos. A sua importância impõe a adoção de todas as medidas adequadas para que a sua atuação seja sempre a melhor possível, com a maior eficiência e menor custos. A nível europeu e a nível nacional, o nosso foco nesta dissertação, foram adotadas medidas que levaram progressivamente a uma maior aplicabilidade de meios digitais em direção a uma unificação entre as Administrações Públicas dos diferentes Estados assim como a uma maior interligação entre os diferentes serviços públicos nacionais. A interoperabilidade que começou a existir entre os serviços públicos de um Estado e ao mesmo tempo entre estes e os serviços de outros Estados

da União Europeia criou uma administração pública em linha a nível europeu e nacional em cada Estado.

O assumir da nova realidade digital dos serviços públicos da União Europeia e dos Estados, dada a dimensão da interoperabilidade e do número de dados que passaram a circular, impõe que haja a perceção de quem assumirá a responsabilidade quando, apesar das normas criadas e recomendações elaboradas, haja o desrespeito pelo que se estabeleceu nos diversos diplomas criados em matéria de proteção de dados e aplicação de meios tecnológicos nos serviços públicos. A partilha indevida dos dados ou a utilização dos dados para finalidades não consentidas pelo titular dos dados são alguns dos problemas que podem resultar da adoção de meios digitais, numa dimensão europeia e nacional, na proporção que ocorre. Com a ligação que se estabelece entre países diferentes, cidades diferentes dentro de um determinado país e entre serviços da mesma cidade, torna-se imperativo saber qual o procedimento caso algum inconveniente ocorrer relativamente aos dados partilhados pelos cidadãos. Se a evolução é necessária e tem que ocorrer a verdade é que apenas pode ocorrer com a definição concreta e direta de quem assumirá a responsabilidade nos casos de incumprimento das normas. O respeito das normas e dos princípios, como o princípio da lealdade e o princípio da segurança, tem que ser acompanhado com a definição concreta, para todos os casos, de quem irá assumir a responsabilidade no caso de a segurança dos dados deixar momentaneamente de existir. O problema que existe nesta matéria é que apesar dos esforços para a definição do responsável pelo tratamento de dados e de como as suas funções tem que ser desempenhadas na proteção dos dados pessoais que lhe são confiados, a verdade é a indefinição ainda persiste. A modificação ocorrida de uma heterorregulação para uma autorregulação veio diminuir os entraves que estavam a existir, mas veio representar a criação de áreas cinzentas em que verdadeiramente se questiona quem regula determinado caso ou ato concreto.

1. A digitalização

A sociedade encontra-se em transição/transformação digital¹, permanente e num caminho sem retorno, em direção ao que se projeta ser uma sociedade cada vez mais desenvolvida e direcionada para o futuro. Tem que haver a consideração deste tópico tendo presente que a digitalização é o recurso feito a qualquer instrumento tecnológico em substituição de recursos humanos e que vem permitir que haja uma conectividade imediata entre pontos diferentes, administrações públicas diferentes, serviços públicos diferentes, entre outras vertentes que podem e recorrem a meios tecnológicos. As tecnologias estão em permanente evolução, sendo neste sentido, como que uma fonte permanente de meios que permitem o desenvolvimento e melhoramento da realidade e a resolução de uma forma mais eficaz dos problemas que vão surgindo. Houve um crescente reconhecimento de que as tecnologias fazem a diferença na realidade social e permitem alcançar novos marcos de desenvolvimento que vêm de certo modo permitir a existência de um leque de novas soluções para os problemas existentes.

A digitalização começou, deste modo, a ser uma das prioridades estabelecidas pela União Europeia e pelos Estados-Membros, assim como das restantes potências mundiais como os Estados Unidos da América², ao perceberem que o recurso a um determinado instrumento tecnológico levava a uma simplificação administrativa e tributária de determinados atos, a uma redução de custos e tempo para o Estado, cidadãos e empresas e a uma maior facilidade de comunicação entre serviços públicos. O que se consegue visualizar com a transformação que se vai introduzindo e dominando todos os aspetos de uma sociedade é de tal forma positivo e benéfico que não pode ser negado e limitado por uma sociedade com recursos para evoluir e atingir novas formas de comunicação. Os benefícios que se começam a evidenciar com a primeira utilização de forma significativa das tecnologias é a motivação para a aposta na digitalização de uma forma consistente e coesa.

Existem benefícios³ que são significativos e essenciais às necessidades dos cidadãos⁴⁵ e é nisto que se tem de centrar os governos e a União Europeia para que os efeitos que começam a ser reconhecidos com a aplicação de meios tecnológicos seja ainda mais justificada e o

¹ Nesse sentido, cfr. DELGADO, Isaac Martín, "El acceso electrónico a los servicios públicos: hacia un modelo de administración digital auténticamente inovador", in *Sociedad Digital y Derecho*, Imprensa Nacional del Boletín Oficial del Estado, 2018.

² <https://americaninnovators.com/digitaltransformation/>.

³ A vida dos cidadãos começa a ser dominada pelas tecnologias e há a criação de uma certa dependência nos benefícios que começam a ser sentidos. Uma vida sem tecnologia começa a não ser aquela que se ambiciona e projeta como o futuro próximo.

⁴ FONSECA, Isabel Celeste, "Governança Pública (Local) Digital: notas breves sobre a estratégia em curso de aceleração da transição digital", in Artur Flaminio da Silva (coord.), *Direito Administrativo e Tecnologia*, Coimbra, Almedina, 2021, páginas 29-57.

⁵ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_pt.

investimento económico necessário possa a ser visto como viável. A digitalização impõe uma permanente avaliação destes benefícios e a ponderação dos mesmos com os riscos que dela também advém, tendo sempre de haver um equilíbrio entre o que se espera alcançar e os riscos que essa tentativa irá significar. Os direitos fundamentais dos cidadãos não podem ser postos em causa com a aplicação de um meio tecnológico apenas por significar uma diminuição dos custos. O caminho da transformação digital tem de ser feito sempre de uma forma ponderada de modo a que possam ser feitas as escolhas das medidas adequadas e justificativas para o que se quer atingir. A existência prévia de apenas documentos físicos não significava que não existam esses mesmos riscos, o que diferencia é a sua magnitude quer em termos de quantidade de dados pessoais quer em termos de facilidade e velocidade em que os mesmos podem ocorrer. Com a digitalização há riscos que passam a existir, há um maior número de dados pessoais que passam a circular entre dois pontos diferentes e consequentemente a probabilidade de um determinado meio tecnológico não funcionar e bloquear a prática de atos necessários ou de haver uma partilha indevida existem e tem que ser considerados, representando deste modo um risco para a segurança dos dados pessoais partilhados e confiados pelos titulares dos dados pessoais.

1.1. A digitalização e a sua evolução

A consciencialização da potencialidade da digitalização leva a que haja uma necessidade de programação de cada Estado e da União Europeia⁶ que venha permitir uma evolução contínua, ponderada e correspondente aos interesses e necessidades dos cidadãos e dos Estados. Neste sentido são criados programas/planos que delimitam a cronologia adequada à realidade digital em termos do que e como se quer atingir no futuro, do que já existe em termos de meios tecnológicos, o ponto de situação em termos de aplicabilidade destes mesmos meios e o que se poderá ambicionar para o futuro, assim como agendas digitais e estudos sobre o que pode ser melhorado e de como os programas/planos criados estão a ter efeitos práticos e de que modo o seguinte terá de ter isso em consideração. A evolução que se tem registado tem sido sempre feita de uma forma progressiva e no caminho e entendimento de que apenas com uma ponderação do que se pode fazer e do que pode evoluir é que se consegue avançar de programa em programa ou de plano em plano de uma forma que se revele proveitosa em termos de

⁶ https://www.europarl.europa.eu/pdfs/news/expert/2021/4/story/20210414STO02010/20210414STO02010_pt.pdf.

aproveitamento de todas as vantagens que podem ser adquiridas com um determinado meio tecnológico.

A nível europeu o caminho da digitalização começou com a percepção de que os Estados-Membros recorriam à tecnologia na sua atuação no mercado interno mesmo antes de haver alguma regulação legislativa europeia e sem que existissem programas definidos que fossem ao encontro do que seria o melhor aproveitamento dos meios existentes tendo em conta as finalidades adequadas⁷⁸. Havia, ainda, uma desigualdade quanto à capacidade de investimento em meios tecnológicos levando, deste modo, a pouca igualdade em termos de desenvolvimento e harmonização quanto ao nível de tecnologia utilizada, o que fazia com que o recurso à tecnologia não estivesse a ter os benefícios que poderia ter com os recursos económicos europeus. Não havendo uma base comum a todos os Estados não é possível haver uma evolução como Estado e como União e consequentemente há um desperdício de recursos resultante do facto de que não se encontrarem todos ao mesmo nível em termos de desenvolvimento tecnológico e aplicação dos recursos existentes. Reconheceu-se, nesse sentido, à Comissão Europeia o papel de criadora desta base comum através de iniciativas que permitissem que esta aposta no digital ocorresse de uma forma generalizada e ao mesmo nível entre os Estados. Esta competência, assumida pela Comissão, partilhada entre a União Europeia e os Estados-Membros deriva da previsão legal dos artigos 4.º, n.º 2, alínea a) e 2.º, n.º 2 do Tratado sobre o Funcionamento da União Europeia (TFUE). Preveem estas normas que o reconhecimento aos Estados de autonomia ocorre sempre até ao momento em que se reconhece que é necessária a intervenção da União para agir naquilo que os Estados não estão a agir. Os Estados são quem tem a iniciativa e a liberdade de atuação, sendo apenas da competência da União na medida do que se considerar que está a ser feita de forma insuficiente.

A criação de um espaço comum em que os cidadãos possam circular sem limitação não fundamentada ou com inconvenientes desnecessários deve ser o objetivo que resume o interesse e investimento de recursos que é feito pela União sempre que reúne esforços para melhorar a sua atuação como um todo e a qualidade de vida dos seus cidadãos. Todos os caminhos traçados

⁷ ABREU, Joana Covelo de “Os princípios gerais da Administração Pública em linha na União Europeia e a análise do artigo 14.º do CPA – revisitando as necessidades de literacia digital” in Carla Amado Gomes *et al.* (ed.), *Comentários ao Código do Procedimento Administrativo*, Lisboa, AAFDL, volume I, 2023, páginas 2 e 3.

⁸ Subentendem-se como finalidades adequadas todas aquelas que são definidas no sentido de melhoramento da utilização dos meios existentes e que definem o que se pretende alcançar no futuro. As finalidades para serem consideradas como adequadas tem que também ter em consideração a capacidade de investimento de cada Estado e de que forma precisam de modificar a sua realidade para cumprir com o delimitado pela União nos seus programas/planos.

pela União devem ser feitos para que haja uma circulação mais fácil, incentivadora e sem elementos que possam de alguma forma condicionar a liberdade que se reconhece e ambiciona. Tratando-se de criar os elementos para a existência de um espaço sem fronteiras entre os seus Estados-Membros, a União Europeia tem de facilitar, assim e centralizando o tópico da digitalização na Administração Pública, no contexto da prestação de serviços públicos, uma interoperabilidade de dados (pessoais e não pessoais) entre as entidades públicas congéneres dos Estados-Membros e as instituições, órgãos e organismos da União envolvidos. Só assim os cidadãos se sentem efetivamente motivados a exercer as liberdades de circulação.

1.2. Digitalização e a Administração Pública

A digitalização, como foi adiantado previamente, abrange toda a sociedade sem fazer discriminação quanto ao que se pode aplicar e aos setores que podem beneficiar das alterações positivas que da mesma derivam. A Administração Pública não se exclui desse âmbito e rapidamente se entendeu que a evolução dela e a prestação de serviços mais próximos do cidadão passaria por soluções tecnológicas que ligariam de forma mais efetiva os cidadãos ao Estado. Surge, deste modo, a possibilidade de existir uma Administração Pública Digital, também denominada por autores como Miguel Prata Roque como Administração Eletrónica, em que a tecnologia assume um papel importante e vem transformar tudo o que até então era praticado. Os serviços públicos assumem deste modo uma vertente digital e começam a transformar a prestação de serviços aos cidadãos e empresas mais prática, simples e com uma maior conectividade. Ao puderem ser praticados à distância, o que revoluciona de uma forma positiva o acesso aos serviços públicos, vem significar para além da sua melhoria, uma diminuição dos custos que representam para um Governo e possibilitar que os meios que existem numa sociedade, em termos de recursos humanos e monetários, possam ser aproveitados de uma melhor forma e, conseqüentemente, aumentado a sua efetividade. A tecnologia já existia nos serviços públicos, mas não era utilizada como meio de substituição de atos praticados por humanos por máquinas, mas sim como um meio que ajudava o ser humano a praticar esses mesmos atos. O registo numa plataforma de determinados atos é uma forma de recorrer à tecnologia, mas que não se equipara à criação de uma plataforma que une diversos serviços públicos prestados em locais diferentes como ocorre, a título de exemplo, na saúde.

A evolução que se tem registado na Administração Pública resulta de estudos⁹ sobre a potencialidade das tecnologias e de qual seria o melhor proveito dos recursos existentes assim como o estabelecimento de metas realistas face àquilo que pode ser investido pelo Estado de forma a tornar este cada vez mais ligado com os seus cidadãos e com maior capacidade de correspondência com o que estes precisam e ambicionam¹⁰. Esta compreensão da realidade tem que ser feita sempre que se considerar pertinente de modo a que haja uma atuação concertada com o que se pretende e consegue evoluir. Não é suficiente haver uma ambição daquilo que não se consegue atingir ou do que dificilmente se vai conseguir concretizar.

A pandemia que todos vivemos, associada à Covid-19, foi a demonstração ideal de que a Administração Pública já se encontrava a dar passos decisivos em termos digitais, embora um longo caminho ainda tivesse de ser percorrido, e que a presença da tecnologia já existia e era aplicada¹¹. Os serviços públicos continuaram em funcionamento, dentro das limitações inerentes ao período que atravessávamos, e permitiram que a sociedade continuasse a ter acesso aos mesmos serviços que tinha, contudo, através maioritariamente de um único formato, o formato digital¹². Nem todos os serviços se encontravam preparados para a modificação inesperada e repentina do seu modo de exercício e, por este motivo, encontraram dificuldades práticas nos serviços que prestaram à população. Foi, noutro sentido, uma forma de testar até que ponto poderia a tecnologia interferir na relação que se estabelece entre o Estado e a população e de que modo pode essa mesma tecnologia ser utilizada para desempenhar o papel que aquele tem perante esta¹³.

A digitalização veio simplificar a Administração Pública e desprendê-la de meios e mecanismos que não conseguem corresponder da melhor forma possível, como outrora o fizeram, às necessidades dos cidadãos¹⁴, e veio, por outro lado, pôr em ênfase na importância da existência de uma administração pública cada vez mais aberta e capaz de permitir que todos

⁹ Foi criada na União um Centro responsável em matéria de aplicabilidade de tecnologias que dá um apoio aos Estados sobre o que se pode ambicionar no futuro e quais serão as melhores estratégias e políticas a adotar. Para mais informações pode ser consultado https://knowledge4policy.ec.europa.eu/foresight/digital-transformation-public-administration-services_en.

¹⁰ https://knowledge4policy.ec.europa.eu/foresight/digital-transformation-public-administration-services_en.

¹¹ A pandemia veio colocar ênfase na realidade digital existente e nas fragilidades que existiam. Com a necessidade inesperada dos recursos tecnológicos foi facilitada a perceção de que ainda haveria muitas coisas a serem melhoradas e investimento a fazer para se conseguir ter serviços públicos digitais com meios suficientes de resposta.

¹² SILVA, Artur Flaminio, "Inteligência Artificial e Direito Administrativo", in Artur Flaminio Silva (dir.), *Direito Administrativo e Tecnologia*, 2ª Edição, Coimbra, Almedina, 2021, página 10.

¹³ ALVES, Joel A. – "Administração eletrónica, eficiência e proteção de dados: breves considerações à luz dos princípios gerais da atividade administrativa", in PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.). *Anuário da Proteção de Dados 2022*. Lisboa: CEDIS, 2022.

¹⁴ SANTOS, Helena Patricia Neves dos, "Administração eletrónica local: análise sobre a modernização da administração local e respetivos desafios", in Isabel Celeste M. Fonseca (dir.), *Governança Pública Digital, Smart Cities e Privacidade*, 1ª Edição, Coimbra, Almedina, 2022, páginas 127 a 147.

os cidadãos tenham e consigam exercer o direito de aceder aos seus dados e informações pessoais sempre que assim entenderem e de uma forma mais fácil e acessível. Com o recurso à tecnologia é possível que de forma mais direta possam os cidadãos aceder aos seus dados e alterá-los sempre que assim se justificar no exercício do seu direito de retificação previsto no artigo 16.º do RGPD. Este acesso e alteração já existia antes, mas a facilidade com que passou a existir é uma novidade que surge com a utilização de tecnologias.

A perspetivação de uma Administração Pública Digital tem, contudo, de ser feita sem que sigamos a falácia de considerar que a transição digital vai abranger a totalidade da sociedade no momento de utilização dos meios tecnológicos. Os meios digitais em si não são discriminatórios, mas a verdade é que na sua aplicação prática acabam por não conseguirem ser utilizados por todos os cidadãos de igual forma. Não pode ser entendido pela Administração Pública que os seus serviços podem ser todos integralmente e completamente digitais e esperar que os cidadãos com pouco conhecimento de tecnologias ou muito limitado acesso a meios digitais ou sem acesso e conhecimento, como são as pessoas com mais idade, possam de algum modo serem esquecidos ou desvalorizados. A existência e a necessidade de evolução não podem se considerar como universal, abrangente e justificativa para haver discriminação ou uma diminuição das exigências que se impõe aos serviços públicos praticados de forma física¹⁵. Todos os cidadãos têm que ter acesso à Administração Pública independentemente da evolução da mesma e sempre dos mesmos modos, não podendo haver uma diferenciação de exigência de acordo com a forma como os serviços são prestados. A prestação de serviços à distância tem que ser pautada pelo mesmo rigor que a prestação em cada serviço público presencialmente.

A existência de meios tecnológicos no seio da Administração Pública veio criar a possibilidade de os serviços públicos de cada país terem como se ligar uns com os outros e trabalharem em conjunto no sentido de uma atuação mais facilitada e interligada. Se um serviço público apenas tem a responsabilidade de praticar parte do que o cidadão necessita, é desejável que aproveite os meios tecnológicos para comunicar com outro serviço público de modo a que seja possibilitado ao cidadão o respeito pelos seus interesses sem que tenha de comunicar todos os dados novamente. É neste sentido que surge o termo interoperabilidade. Esta interoperabilidade, referida já previamente, leva a falar da administração em linha¹⁶, que surge como a concretização

¹⁵ BRANDÃO, Ana Paula *et al.* (eds.) - *Enciclopédia da União Europeia*, Lisboa, Petrony, 2017.

¹⁶ A União Europeia tem demonstrado a necessidade de os Estados e a própria União apostarem numa interligação entre si, entre os seus serviços e entre os serviços dentro de cada Estado. Tem neste sentido adotado algumas estratégias e atos que tem como objetivo orientar os Estados no melhor sentido possível. Para mais informações pode ser consultado <https://digital-strategy.ec.europa.eu/en/policies/egovernment>.

da aplicabilidade da interoperabilidade nos serviços públicos da Administração Pública. A interligação criada possibilita a prestação única de uma determinada informação, princípio da declaração única ou da uma única vez (once-only principle), ao invés de ter de ser prestada sempre que necessário, através de uma comunicação entre serviços e Administrações Públicas. Com esta comunicação surge uma Administração Pública diferente da que tínhamos até então, interligada entre si, nas suas variadas vertentes, através de “um fio condutor” que permite menos burocracia, mais simplicidade nos procedimentos e serviços que tem para oferecer ao cidadão e empresas e consequentemente mais capacidade de resposta dada às necessidades de cada cidadão e/ou empresa.

1.2.1. A digitalização da Administração Pública na União Europeia

Quanto à aposta na digitalização na Administração Pública na União Europeia houve a delimitação, através da iniciativa da Comissão Europeia, de um plano de criação de uma administração pública em linha entre os Estados que vem permitir que haja a constituição de uma comunicação/interligação entre os serviços públicos europeus. A prestação de serviços públicos aos cidadãos europeus ocorre independentemente da nacionalidade do cidadão, ou seja, a prestação de um serviço a um cidadão num determinado Estado-Membro não tem em consideração se esse cidadão é daquele Estado ou se é natural de outro Estado. Sempre foi assim, contudo, com o surgimento da aplicabilidade da tecnologia, cedo se percebeu que a burocracia e os custos que existiam poderiam ser facilmente reduzidos e assim deste modo tornar o acesso de um cidadão de outro Estado mais motivante com a redução dos entraves territoriais. Um cidadão que prestasse informações suas no seu Estado tinha de o fazer novamente no Estado a que se dirigia e nesse sentido era uma limitação para a efetividade da prestação de serviços. Com a criação de uma administração pública em linha no seio da União Europeia, houve a criação de um fio condutor entre os serviços dos diferentes Estados e uma interoperabilidade entre os mesmos.

Esta interoperabilidade, e consequente administração em linha, foi sendo criada dentro de cada Estado, sendo o desafio a criação de um alinhamento de entendimentos dos diferentes Governos dos Estados. Todos os Estados têm a sua autonomia reconhecida, a sua soberania nacional, com a adesão à União Europeia, mas no fundo todos querem que haja uma comunicação entre todos de modo a que possam também beneficiar da circulação dos seus cidadãos. A interoperabilidade que deriva de uma administração pública em linha, como vimos

anteriormente, começou a ser perspectivada como uma oportunidade de desenvolvimento com vantagens inegáveis e que apenas beneficiariam cidadãos e empresas. A União Europeia tem se revelado um importante motor em matéria da digitalização dos serviços públicos ao adotar diversos projetos, atos, planos e recomendações sobre o modo como deve a União Europeia atingir de forma planeada e estruturada novos patamares de desenvolvimento que permitam alcançar consideráveis vantagens para os Estados-Membros e respetivas Administrações Públicas. A Comissão Europeia tem trabalhado no sentido de compreender o que o mercado precisa e de que modo cada Estado tem acompanhado as necessidades e nova realidade que a digitalização dos serviços públicos requer e de que forma necessita de um apoio europeu. A evolução organizada e delimitada de acordo com as necessidades dos cidadãos europeus é essencial para a compreensão de tudo aquilo que tem de ser trabalhado, quais as fragilidades que se verificam e que riscos têm de ser equacionados no planeamento de novos avanços nesta matéria.

Um dos programas que está neste momento em vigor é o Programa Europa Digital¹⁷ que visa contribuir para que as economias europeias sejam cada vez mais competitivas em termos de tecnologia e atinjam níveis de progressão cada vez mais elevados, tendo sido este programa o primeiro a ser um apoio financeiro para a promoção do desenvolvimento dos cidadãos e das empresas no sentido digital e contribuir para que fosse dado o investimento inicial necessário para que a digitalização pudesse ser posta em prática. Por ter sido o primeiro merece o destaque e menção face aos outros programas adotados. Podemos juntar a este programa o Guião para a Década Digital que estabelece o quadro de governação para alcançar os objetivos em matéria digital até 2030 ao definir as linhas condutoras a ser tidas em consideração quando praticados atos governamentais. Para que haja estes programas é importante que haja um índice como o Índice de Digitalidade da Economia e da Sociedade (IDES), criado pela Comissão Europeia em 2014, que visa analisar através de um relatório a competitividade digital dos Estados-Membros entre si e a evolução de cada um ao longo dos anos¹⁸. Através deste índice tornou-se possível perceber quais os Estados que tinham de ter mais apoio na aposta na digitalização de modo a acompanhar, dentro do possível, o mesmo nível os restantes Estados-Membros. Ao longo dos

¹⁷ <https://eurocid.mne.gov.pt/europa-digital>.

¹⁸ O IDES foi criado em 2014 e é elaborado todos os anos. É um instrumento que visa analisar a evolução da União Europeia nesta matéria e, por outro lado, analisar o progresso de cada Estado-Membro em termos digitais. É um relatório que se foca, deste modo, não apenas na União Europeia e nas suas instituições, mas também nos Estados em específico. Nem todos os Estados tem o mesmo número de recursos e por este motivo nem todos progredem ao mesmo ritmo. Todas as informações relativas ao índice mencionado podem ser consultadas em <https://digital-strategy.ec.europa.eu/en/policies/desi>.

anos temos assistido a uma evolução significativa do índice mencionado, perspetivando-se que assim continue à medida que se aposta mais na digitalização e se abra novos horizontes. Estamos perante, como tem sido afluído, de uma verdadeira e extensiva transformação digital da Administração Pública que requer um acompanhamento a todos os níveis da sociedade e um esforço de todos cidadãos de modo a que se consiga passar da teoria para a prática e se concretizar os objetivos estabelecidos.

Neste âmbito tem que ser destacada uma plataforma que vem trazer uma maior colaboração entre os Estados-Membros ao disponibilizar informações sobre acontecimentos recentes em matéria de administração em linha e interoperabilidade e que permitem que haja uma cooperação constante de notícias e eventos que podem ajudar outros Estados na reunião de informações úteis e no solucionamento de alguma dúvida que possa existir. Conjuntamente foi criada a plataforma JOIN UP¹⁹ que é um ponto de comunicação que se estabelece entre os Estados e que tem em vista o cumprimento da política de interoperabilidade e a demonstração aos Governos de soluções digitais para os problemas que possam existir ou ideias que possam precisar para evoluir digitalmente. É um espaço de conhecimento e de troca de informações que possam de alguma forma ser úteis. Para além dos eventos e notícias que a plataforma disponibiliza a verdade é que estes precisam que haja um meio mais direto de partilha de informações que permitam uma maior interoperabilidade entre os serviços públicos e o combate a qualquer fragilidade que a possa limitar. todos os meios que possam ajudar a pôr as políticas em prática, a passar da previsão legal para a prática, devem ser vistas com bons olhos.

Todos estes instrumentos tem um objetivo principal de criar uma sociedade digital com as bases necessárias para que os seus interesses possam ser respondidos de uma forma progressivamente mais simplificada, mas, sem que com isso, haja uma diminuição da qualidade dos serviços prestados. Todos os instrumentos mencionados a nível europeu devem ser acompanhados e integrados em cada Estado-Membro através de programas nacionais se assim se revelar adequado.

1.2.2. Programas a nível nacional

O nosso país foi adotando os programas, recomendações e orientações emanadas pela União Europeia de modo a adaptar-se e evoluir no sentido da digitalização da sua Administração

¹⁹ Podemos falar da iniciativa da Comissão de criar uma Europa Interoperativa. Foi criado para o efeito uma plataforma que pode ser consultada em <https://joinup.ec.europa.eu/>.

Pública e a definição do que deve e precisa de ser feito. Quando avaliada a evolução que fomos registando podemos constatar que o nosso país se encontra ainda em 15º lugar dentro dos 27²⁰ Estados-Membros em termos de desenvolvimento e aposta na digitalização, o que demonstra que apesar do esforço feito ainda existe um longo caminho para a frente e que a aposta nos meios digitais deve continuar a existir e a ser reforçada. Registou-se uma evolução desde 2021, com a subida de uma posição (que era o 16º lugar), contudo, ainda não temos a qualificação igual, pelo menos, à média europeia que se encontra consideravelmente acima, mas que pode ser vista como o incentivo e referência na continuação do trabalho nesta matéria e com a demonstração de que há resultados com as políticas que já foram adotadas e que continuam em vigor. Todos os programas que foram sendo adotados pela União, tais como, a Estratégia para a Transformação Digital da Administração Pública 2021-2026²¹ ou o Plano de Ação Transversal de 2020-2023²², encontram-se atualmente em vigor de modo a contribuir para que o nosso país evolua nesta matéria e alcance um IDES superior a cada ano que passa²³. A transformação da sociedade portuguesa em matéria jurídica, económica, política e social tem imposto um investimento económico, mas tem também significado alterações que permitem que haja vantagens reconhecidas aos cidadãos e que permitem que a justiça portuguesa consiga ser mais eficiente e corresponsiva ao que se espera ser. Uma justiça mais ágil, menos burocrática e com mais capacidade de resposta para os problemas que surjam e para a concretização de projetos e ambições dos seus cidadãos.

Em termos de programas podemos destacar o programa SIMPLEX²⁴, criado em 2006, que tem como objetivo principal a simplificação da Administração Pública quer em benefício dos cidadãos com um acesso mais direto e simples quer para a prestação do serviço público de uma forma mais próxima do cidadão e com uma maior efetividade. Este programa foi reforçado em

²⁰ Foi no ano de 2022 que se registou este IDES podendo o mesmo ser consultado em <https://digital-strategy.ec.europa.eu/en/policies/digital-portugal>. Neste relatório podemos constatar que a avaliação feita ao nosso país e o que foi tido em consideração para a avaliação do ponto de situação do nosso índice.

²¹ Esta estratégia estabelece que “pretende contribuir para uma administração pública mais digital, que disponibilize melhores serviços e com maior valor acrescentado, estando mais perto dos cidadãos e das empresas”. Podemos consultar, de modo a obtermos mais informações o seguinte endereço <https://www.portugal.gov.pt/pt/gc22/comunicacao/noticia?i=governo-aprova-estrategia-para-a-transformacao-digital-da-administracao-publica-2021-2026>.

²² Este plano integra os contributos de todas as áreas governativas de modo a produzir diversos instrumentos para fomentar a mudança e apoiar a Administração Pública (AP). Este apoio é concretizado através de um processo de adoção de soluções cloud pelo Conselho para as Tecnologias de Informação e Comunicação na Administração Pública (CTIC), por atribuição por parte do Estado a este Conselho. Toda a informação relativa a este Plano pode ser consultada em <https://tic.gov.pt/documents/37177/280325/Plano+de+A%C3%A7%C3%A3o+Transversal+para+a+Transforma%C3%A7%C3%A3o+Digital+da+AP+2021-2023.pdf/1a8bdefc-ad29-e7a9-898c-d21f55cbea7b>.

²³ Estes dados são criados pela Comissão Europeia que todos os anos analisa como é que se encontra o Índice de Digitalidade da Economia e da Sociedade em cada Estado-Membro para poder assim orientá-los nos melhores meios de concretização mais ativa da digitalização. Em concreto, podemos analisar o que a Comissão concluiu na sua análise sobre o nosso país através do documento presente em <https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance>.

²⁴ <https://www.simpler.gov.pt/>.

2016 e vai se adaptando nas suas medidas ao longo dos anos para que possa atingir novos objetivos no sentido de melhoria das finalidades para as quais foi criado e que foram mencionadas anteriormente. Em termos de medidas podemos destacar as que se centraram na melhoria dos contratos públicos com a obrigatoriedade, desde 2009, de os contratos públicos serem eletrónicos. de modo a que todos os contratos públicos que tenham de ser do conhecimento dos interessados e que tenham de ser, deste modo, publicitados pelas entidades adjudicantes através da sua publicação no Portal dos Contratos Públicos (Portal Base). Com esta abertura a um acesso simplificado aos contratos públicos estamos perante transparência, simplificação, democracia e reconhecimento de que pode haver uma discordância quanto, por exemplo, ao resultado de um determinado concurso. Com um acesso mais direto há a possibilidade de haver um melhor exercício de direitos²⁵.

A análise que é feita ao nosso país através do IDES é de extrema importância para pudermos perceber o que é necessário ainda adotar e em que medida estão os programas e planos a ser eficazes no seu objetivo e como estão os recursos criados a ser interpretados na prática, por outras palavras, se estes estão a ser vistos como um fator benéfico e diferenciador ou se os riscos e custo que representam não compensa os benefícios que estão a existir. Sem o índice acabamos por não ter a perceção sobre se a evolução ocorreu, ou se, pelo contrário o nosso país se encontra estagnado ou praticamente estagnado nesta matéria e em que sentido temos de modificar o que tem vindo a ser feito. Vemos que apesar de este índice estar abaixo da média da União Europeia a verdade é que já existem, como foi referido anteriormente, demonstrações de efeitos positivos e com impacto na Administração Pública com o melhor acesso aos serviços públicos, melhor prestação dos mesmos e a redução dos custos com a prestação de um serviço. A Agência para a Modernização Administrativa (AMA), foi criada nesse sentido, sendo uma plataforma atualizada de forma a regular através os dados disponibilizados no portal nacional de dados abertos da responsabilidade das entidades com competência e responsabilidade para tal. Esta plataforma reúne informações sobre vários setores/temas que compõem a Administração Pública, tais como, dados públicos portugueses, através da plataforma dados.gov²⁶, contratação

²⁵ https://repositorium.sdum.uminho.pt/bitstream/1822/71364/1/relatorio_etica.direito2020_observatoriociberseguranca_cnacs.pdf.

²⁶ Quando falamos nos dados públicos portugueses torna-se claro que é uma plataforma que permite que haja um acesso a todos os dados indicadores de como se encontra a nossa sociedade em vários temas e segundo determinadas estatísticas.

pública, através da plataforma base.gov²⁷, saúde, através da plataforma sns.gov²⁸, justiça, através da plataforma partilha.justica.gov²⁹, e turismo, através da plataforma dadosabertos.turismodeportugal³⁰. A criação de uma base comunicativa como a AMA permite que haja um conhecimento esclarecedor sobre o que se tem adotado em matéria de digitalização da Administração Pública, interoperabilidade e administração em linha, tudo no mesmo “lugar” e o que pode ser exigido como próximos passos a adotar.

Tudo o que foi criado até aos dias de hoje para ajudar a Administração Pública a se tornar mais próxima dos seus cidadãos através de serviços públicos capazes de corresponder às suas necessidades, foram de importantíssimo relevo para que hoje possamos ter em Portugal uma interoperabilidade entre os serviços públicos com todos os instrumentos necessários para criar uma administração pública em linha que é funcional e respeita a transparência e a facilidade de acesso e comunicação entre os principais interessados no Estado, os cidadãos. Apenas com um planeamento adequado e com a aplicação das medidas proporcionais e adequadas podemos ter uma Administração Pública ao serviço dos seus cidadãos.

1.3. Principais problemáticas da digitalização

O entusiasmo pela digitalização, que se tem assistido nos últimos anos por parte dos titulares dos dados e por quem trabalha em serviços públicos, não deve conduzir a uma ignorância de que, apesar de significativamente melhorar o acesso a serviços públicos, implica, ao mesmo tempo, que determinados incidentes possam ocorrer³¹. Os problemas, que advêm da quantidade de dados que são partilhados, podem existir devido a diversos motivos podendo ser resumidos, numa tentativa que pode ser demasiada redutora e generalista, à partilha indevida dos dados, ao tratamento desadequado à quantidade e/ou complexidade dos dados partilhados e ao desrespeito pelas finalidades estabelecidas no registo de atividades de tratamento e segundo as quais o titular concordou na partilha dos seus dados. A existência de problemas pode fazer com

²⁷ Foi criada em 2008. Desde 1 de novembro de 2009 que todos os contratos públicos são adjudicados eletronicamente, através de plataformas eletrónicas, há apenas a exceção dos ajustes diretos, sendo previsto no Código dos Contratos Públicos no artigo 133.º que há uma publicação das peças do procedimento de um determinado concurso para um contrato público na plataforma própria, o base.gov. Com esta disponibilização há uma maior transparência e clareza dos concursos que se encontram a decorrer e quais os requisitos do mesmo e permite deste modo que que tenha intenções de nele participar o possa fazer com base num conhecimento mais acessível e claro.

²⁸ Foi criada em 2011 com o objetivo de facilitar aos cidadãos o acesso a prescrições médicas e a outros dados sobre a sua saúde.

²⁹ Através desta plataforma é possível ter acesso a dados e estatística sobre a justiça.

³⁰ Esta plataforma foi criada com o objetivo de criar uma base de dados sobre as informações essenciais para um turista quando decide viajar para um determinado local, desde o alojamento a atividades que podem ser praticadas e que possam ser interessantes para o turista. É um guia que ajuda o turista através da reunião numa única plataforma dos dados principais sobre um determinado local.

³¹ Quando concordamos com a partilha dos nossos dados fazemo-lo com o conhecimento de que os mesmos serão utilizados para uma determinada finalidade ou para um conjunto delimitado de finalidades. A partilha ocorre de uma forma informada e é este conhecimento que nos permite aceitar e querer que ocorra. Se os dados forem utilizados para outras finalidades não podemos dizer que é uma partilha consciente e consequentemente podemos assumir que se o titular soubesse poderia não quer partilhar os dados.

que pareça improdutivo todo o investimento que se faz para que os meios digitais existam e faz com que os benefícios, cuja existência é inquestionável, possam rapidamente ser desconsiderados face aos problemas que levantam. Do que estamos a abdicar para termos a tecnologia como realidade na nossa Administração Pública? Temos serviços públicos a serem praticados com mais celeridade, mas a que custo? Com que justificação aceitamos a possibilidade de os nossos direitos serem postos em causa com uma partilha indevida ou com a utilização dos nossos dados pessoais para finalidades com as quais não concordamos? São estas as perguntas que de imediato se colocam e que devem servir de reflexão para os defensores da digitalização e para a perceção de que apesar de trazerem benefícios não são isentos de problemas.

O investimento que é feito nesses mesmos sistemas quer em termos económicos quer em formação de mão-de-obra é fundamento para que quem se assume como responsável pelo tratamento tenha a certeza que a adoção de medidas técnicas e organizativas adequadas é sem dúvida o caminho que deve ser seguido³². Não podemos afirmar que a digitalização é isenta de riscos, que os incidentes nunca ocorrerão, e nesse sentido todos os problemas que podem resultar da digitalização tem que ser tidos em consideração, ser estudados, de modo a que se perceba o que pode ocorrer com a partilha de dados. A existência de problemas é uma realidade e tem que ser tida em consideração aquando a ponderação entre as vantagens e as desvantagens da aplicação das tecnologias.

1.3.1. Problema da proteção de dados

A digitalização avassalou um problema que já existia previamente. A partilha indevida de dados que sempre ocorreu na prestação de serviços presencialmente foi intensificado com o recurso a meios tecnológicos. O recurso à tecnologia envolve a circulação de dados pessoais de uma forma que não ocorria antes e significa uma preocupação acrescida na prestação de serviços públicos digitalmente. Como podemos garantir a proteção dos dados quando estamos perante uma realidade a grande escala que envolve riscos significativos? A probabilidade de a partilha de dados ser feita de forma indevida existe e, mesmo com os mecanismos de controlo e as normas previstas, não é possível dirimir todos os riscos e fazer com que a partilha de dados,

³² Dado o que implica modificar a Administração Pública para uma desafiante realidade que, apesar de ser positiva ou ter intenções positivas pode significar sacrificar a segurança que assumimos como parte dos nossos direitos, tem que ser feita com cautela. Ao mesmo tempo é necessário dar a importância que esta modificação assume e não permitir que seja um impedimento, sendo deste modo necessário que se crie mecanismos de prevenção de riscos e de incidentes que informem os cidadãos de qual deve ser a sua expectativa jurídica sobre o tratamento que deve ser feito pelos responsáveis pelo tratamento relativamente aos seus dados em caso de partilha indevida dos seus dados.

independentemente da sua proporção, seja sempre segura e isenta de riscos, como já foi mencionado anteriormente. Podemos contra-argumentar com o facto de estes riscos já existirem anteriormente com a possibilidade de os documentos físicos poderem ser perdidos ou alguém se apropriar dos mesmos sem o poder fazer, contudo, é falacioso comparar este risco com nível de possibilidade de riscos que existe quando os dados passam a existir e a circular virtualmente.

Os potenciais riscos representam um retrocesso a ser tido em consideração quando são adotados meios tecnológicos num panorama da dimensão da Administração Pública em que a quantidade de dados é muitíssimo elevada e estamos por outro lado a falar de um grau social de responsabilidade do responsável pelo tratamento superior aos outros responsáveis pelo tratamento. Saliente-se, contudo, que a responsabilidade assumida pelo responsável não é discriminada legalmente de acordo com quem a assume, mas são os próprios titulares dos dados que tem uma expectativa superior. Apesar de não podermos não pôr em prática a digitalização devido a estes riscos, não podemos na mesma medida ver com bons olhos a possibilidade de um determinado serviço do Estado com a importância que representa poder ser não o protetor do cidadão, mas sim uma fonte de perigo para o bem preciso que é os direitos dos cidadãos. O Estado como representante dos cidadãos não pode descorar esse papel e se os outros responsáveis pelo tratamento têm que dar o seu o melhor então aquele tem que dar em dobro o seu melhor.

A pandemia que vivemos a partir de 2020 foi o reflexo de que a questão da proteção de dados tem de ser trabalhada de modo a que se consiga, enquanto Estado, proteger os cidadãos e defender os seus direitos fundamentais independentemente das circunstâncias que os rodeiem, mas sem que isso represente desvantagens que se sobreponham ao que se quer atingir. Não podemos ignorar os problemas que daqui advêm e de que modo os cidadãos permitem que os dados sobre a sua vida privada tenham de ser partilhados se querem continuar a ter uma vida em movimento sem ser interrompida ou atrasada por motivos pandémicos. A falta de garantias prestadas ao titular dos dados sobre a capacidade de tratamento e proteção que podem ser prestados, a falta de clareza de quem assumirá a responsabilidade se os dados forem partilhados indevidamente, devido a zonas cinzentas a não ignorar, e a falta de capacidade dos serviços em se adaptar a quem não consegue recorrer aos meios digitais, devem ser o que mais releva quando defendemos que um país digital é a solução para todas as melhorias que

são necessárias³³. Não podemos inconscientemente ignorar que foi o impulso que motivou a que se alcançasse novas metas e objetivos, foi a motivação esperada e necessária e que tornou a pandemia apenas uma justificação parcial da digitalização. É por este motivo necessário haver uma investigação mais aprofundada sobre a proteção de dados de modo a que haja uma previsão legal adequada às novas exigências jurídicas que se impuseram e de modo a que os problemas não se sobreponham aos benefícios.

2. Proteção de dados

A regulamentação da matéria dos dados pessoais tem evoluído ao longo do tempo consoante a tecnologia vai dando os seus passos e a adesão da sociedade à mesma vai crescendo e demonstrando que as vantagens que a mesma proporciona tem que ser tidas em consideração por parte de quem tem o poder de governar a sociedade. O poder legislativo deve acompanhar essa mesma evolução ao ritmo que permita que o progresso seja encarado e posto em prática segundo normas adequadas para o efeito que permitam que assim o seja. Não podemos querer alcançar novos patamares de desenvolvimento se não abriremos os nossos horizontes para que essa evolução aconteça, assim como, e em sentido contrário, não podemos querer que seja feita sem cautela e sem ponderação de qual deve ser o caminho a adotar nesta matéria. A aplicação de novas formas de pensar impõe que haja mecanismos legais para a resolução das questões jurídicas que inevitavelmente irão surgir com a utilização cada vez mais notória dos meios tecnológicos, como vimos anteriormente, para os mais diversos fins e com uma maior circulação de dados pessoais dos cidadãos portugueses e europeus. A pandemia e a inteligência artificial vieram impor uma mudança de pensamento, que veio influenciar e impulsionar o modo como o titular dos dados vê a necessidade de proteger os seus dados pessoais, mas também levar a que, para cumprirem determinado objetivo ou interesse, descorem a importância que os seus dados têm e de que modo ao os partilharem os estão a pôr em causa. É uma dualidade de preocupações que pode ser de difícil articulação e que motiva a uma reflexão por quem tem que tomar decisões e determinar medidas para que possamos evoluir e corresponder às novas necessidades, com precaução, de modo a atingirmos um maior desenvolvimento, mas sem que com isso seja posto em causa o alcançado até então.

³³ CALVÃO, Filipa Urbano – “Os estados de exceção e a proteção de dados pessoais”, in Carla Amado Gomes *et al.* (ed.), *Direito Administrativo de necessidade e de exceção*, Lisboa, AAFDL Editora, 2020.

Em 1995 já era deste modo notório que a matéria da proteção de dados encontrava-se em evolução, e foi este reconhecimento que levou à criação da Diretiva 95/46/CE³⁴ e à determinação com maior rigor do tratamento dos dados pessoais num contexto de digitalização, e que o papel do legislador era invocado para criar uma legislação, neste caso através de uma diretiva, que se centrasse apenas e unicamente na matéria de dados pessoais e que pudesse de algum modo conseguir abranger e prever o desenvolvimento que se estava a verificar. Esta Diretiva estabeleceu os princípios e limites quanto à recolha, utilização e tratamento de dados pessoais sem nunca ter elementos fácticos ou “experiência legislativa” para conseguir prever os casos concretos que iriam ocorrer numa área que se altera de uma forma acelerada e imprevisível e nesse sentido, tal como as restantes leis, decretos-leis, diretivas ou regulamentos, revelou-se aquém da realidade que se começou a revelar. A imposição de normas concretas e inovadoras ao progresso do tratamento dos dados pessoais revelou-se o ponto de partida essencial para que o progresso nesta matéria visse as suas bases a ser constituídas e a se projetar no mundo como o futuro de todos os aspetos de uma sociedade e para que os dados pessoais fossem uma preocupação real e não deixasse de ser visto o problema que os mesmos podem criar se não forem protegidos adequadamente.

Em 2001 surgiu o Regulamento 45/2001/CE do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Se queremos o Mercado Único seja visto como o Mercado Único Digital, uma unificação dos Estados-Membros cada vez mais acentuada e uma maior facilidade de circulação de pessoas, bens e serviços neste espaço, é necessária uma lei que dite o modo como a União, como um todo, se deve comportar em matéria de proteção de dados e como pode se projetar no futuro de modo a acompanhar a evolução natural da vida, das sociedades. O que a diferencia da diretiva mencionada no parágrafo anterior é a quem se dirige, ou seja, a diretiva tem como âmbito de aplicação os Estados-Membros, tendo estes de aplicar na sua legislação e sociedade as normas impostas, enquanto este Regulamento tem como âmbito de aplicação a própria União e todos os órgãos e organismos da União. Não podemos querer que os Estados cumpram regras que nem a União conhece e aplica no seu funcionamento, não faz sentido que se queira crescer como potência mundial e como impulsionadora da Inteligência Artificial se depois não sabe como

³⁴ Como vimos anteriormente esta foi a primeira legislação a reunir em si todas as preocupações e cuidados que existem e devem existir desde o momento em que se cria mecanismos que vão lidar com dados pessoais, desde a partilha dos mesmos até ao momento em que tem que ser destruídos todos os dados pessoais que já não estão a ser utilizados para as finalidades para as quais foram recolhidos.

o fazer sem que perder o controlo dos efeitos que poderá vir a ter com estes novos mecanismos. A própria União lida com dados pessoais no seu funcionamento e nesse sentido tem que ficar abrangida por uma legislação adequada à sua realidade e correspondente com a dimensão da mesma e com a quantidade de dados que poderão circular.

No ano seguinte surgiu uma outra Diretiva, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, sendo deste modo mais específica em comparação com as outras fontes legislativas mencionadas mas que acaba por ser um complemento delas ao abordar o modo como as comunicações eletrónicas devem ser feitas de modo a garantir a proteção de dados pessoais quer no seio do Estados-Membros quer pelos órgãos, organismos e instituições europeias. Tendo que existir comunicação para que haja uma administração em linha e uma interoperabilidade entre os serviços prestados aos cidadãos europeus de diferentes Estados-Membros e sendo estas comunicações complexas e com um risco elevado de significarem uma partilha indevida dos dados tem que haver uma regulamentação que tenha esse fator em consideração. Em casos de violação de dados estabelece esta Diretiva como devem proceder os prestadores de serviços e quais os mínimos que devem ser cumpridos por parte dos responsáveis pelo tratamento de modo a que a privacidade e a confidencialidade sejam sempre garantidas em todas as comunicações que sejam feitas. Foi criada esta Diretiva “em conjunto” com outras diretivas³⁵ centradas em outros pontos ligados às comunicações eletrónicas tendo sido posteriormente este pacote de diretivas completado com outras e com a introdução de recomendações específicas em decorrência da Covid-19.

Por último em 2013, antes do Regulamento atualmente em vigor, surge o Regulamento (UE) n.º 611/2013 da Comissão, de 24 de junho de 2013, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho. Para além da consagração de regras relativamente ao tratamento é importante determinar como é que devem as pessoas reagir em caso de haver a verificação de violação de dados pessoais. Os serviços têm que saber como agir em caso de uma violação de

³⁵ Estamos a falar da Diretiva 2002/20/CE ou Diretiva «Autorização», relativa às autorizações de acesso a redes de comunicações, da Diretiva 2002/19/CE ou Diretiva «Acesso», relativa à determinação de acordos para acesso e/ou interligação de cada Estado a diferentes serviços, no respeito das regras da concorrência estabelecidas no Tratado, da Diretiva 2002/22/CE ou Diretiva «Serviço universal», relativa previsão de regras específicas relativas à prestação de serviços de comunicações eletrónicas na UE, do Regulamento (CE) n.º 1211/2009, que cria o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE), e do Regulamento (UE) n.º 531/2012 relativo do à itinerância nas redes de comunicações móveis públicas da União.

dados ser detetada, mas é de igual importância saberem os utilizadores desses mesmos serviços como podem atuar e reagir em caso de uma violação de dados tenha ocorrido e os seus dados tenham sido partilhados indevidamente.

Em 2016 foi criado 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, que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)³⁶, que veio estabelecer uma atualização da matéria de proteção de dados de forma a ficar mais adequado à evolução de 21 anos que ocorreram. Esta Diretiva não conseguia prover segurança necessária para a partilha dos dados pessoais, havendo uma fragmentação na aplicação das normas em matéria de proteção de dados ao nível da União e a existência de um sentimento negativo generalizado da opinião pública relativamente aos riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. Neste sentido o Regulamento vem tentar dissipar estas inquietações e permitir que haja mais uniformidade na proteção de direitos dos titulares dos dados nos Estados-Membros visto que apenas assim conseguimos ter um espaço comum mais coeso e com mais capacidade de resposta aos riscos que podem existir em matéria de proteção de dados.

2.1. Conceito de dados pessoais

O conceito de dados pessoais está previsto no artigo 4.º, 1) do RGPD determinando que os dados pessoais são a “informação relativa a uma pessoa singular identificada ou identificável”³⁷, procedendo o legislador na parte final do conceito à determinação do que se entende por identificável. Para alguns autores não estamos perante um conceito completamente esclarecedor, apesar da delimitação na segunda parte, quanto ao seu âmbito quer relativamente ao que se entende por dado pessoal quer à questão de saber qual o critério que pode ser usado para delimitar os dados que podem identificar uma determinada pessoa. Consideram que o âmbito do conceito é demasiado amplo, o que se traduz em desentendimentos e consequentemente em uma dificuldade para haver coerência sobre o mesmo dado quando colocadas questões por interpretes diferentes. Podem haver ainda casos em que pôr falta de delimitação do conceito se pode considerar como sendo dados pessoais quando na realidade não reúnem os requisitos. Entendem que com este conceito pouco concretizador pode haver

³⁶ Pode ser consultada em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1667850894976&from=PT>.

³⁷ <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1667850894976&from=PT> página 33.

uma aplicação sem limites e consequentemente a desacreditação do próprio conceito e a sua importância nesta matéria não permite que aceitemos que assim o seja, segundo estes autores.

A legislação é composta por um conjunto de conceitos jurídicos que se espera serem concretos, claros e delimitadores e que se transformem no início, na ponte, da resolução dos casos jurídicos que são colocados em tribunal ou outras instâncias. Se em termos gerais dizemos ser este o ponto de partida, numa matéria como a digitalização e a proteção de dados, nova e com uma maior tendência, por isso, para se modificar com maior frequência e rapidez, torna-se ainda mais urgente e justificável a preocupação com a atualização e acompanhamento da lei das modificações e novas necessidades que vão surgindo e a definição dos conceitos claros na sua delimitação. Pode ser contra-argumentado que é necessário que o âmbito do conceito seja em parte discricionário de modo a que possa abranger e prever uma diversidade de casos concretos que, de outro modo, com um conceito menos amplo, não seriam abrangidos. Os autores a favor da construção linguística do conceito consideram que a incerteza que existe quanto a uma matéria ainda a ser explorada como é a transição digital deve ser protegida por conceitos amplos que possam de certo modo eliminar parte dessa mesma incerteza e contribuir para que possam ser exploradas e investigadas tendo por base uma certeza jurídica³⁸ que é o conceito. Em caso de partilha indevida, consideram ainda que o conceito não pode ser considerado como prejudicial para a definição do que pode ser considerado como dado pessoal nos dados que foram partilhados e/ou acedidos por terceiros.

As questões que se colocam relativamente ao conceito são de facto pertinentes e podem fazer com que na prática casos que não cumpram os requisitos de aplicação do conceito sejam considerados como dados pessoais e pode, noutra perspetiva, induzir em erro as entidades responsáveis pelo tratamento de dados pessoais quanto aos dados que podem ser recolhidos³⁹ e quais os dados que não sendo consideráveis como dados pessoais, ou pelo menos não o deveriam ser, não devem ter tratados como tais. Jurisprudencialmente, através de questões prejudiciais, tem se denotado preocupações e a necessidade de se estabelecer um entendimento mais concreto sobre o âmbito do conceito de dado pessoal através de critérios delimitadores e concretizadores deste. Nem todos os casos juridicamente relevantes são de fácil compreensão e resolução ou com consagração clara e evidente da sua solução jurídica e, nesse sentido, a falta

³⁸ MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais*, Coimbra, Almedina, 2023, página 44.

³⁹ Os considerandos 16 a 21 assim como os artigos 2.º e 3.º, tudo do RGPD, consagram o que se deve entender como âmbito e o que este abrange. Contudo, tal como mencionado, há uma delimitação suscetível de ser usada em demasia e aplicada a casos que não deveria ser aplicada.

de concretização do conceito significa que há uma margem de interpretação discricionária que permite que possa ser aplicado o conceito a um leque de casos jurídicos abrangente, mas que, noutra perspetiva, “abre portas” a um uso excessivo do conceito e a perspetivas diferentes e variadas sobre o mesmo caso e da aplicação do conceito ao mesmo. Quando estamos perante um dispositivo que recolhe determinados dados, como as aplicações que surgiram em alguns países, como Portugal, sobre a Covid-19 e respetivas pessoas infetadas, levanta-se a questão de quem tem a legitimidade para tratar os dados pessoais e de que modo e em que termos o RGPD protege estes casos. A consagração jurisprudencial tem-se relevado fundamental para o esclarecimento das questões que foram surgindo com a aplicação quer da Diretiva quer do Regulamento. Por outro lado, temos verificado que jurisprudencialmente e doutrinariamente o facto de não enquadrarmos determinado dado como sendo um dado pessoal segundo o RGPD isso não significa que não possamos aplicar a lei estadual de modo a proteger o titular desse mesmo dado, o que demonstra que a modificação do âmbito não seria limitadora para a resolução dos casos.

Tem sido invocado em determinados acórdãos que não podemos considerar como negativo o âmbito demasiado abstrato dado que deste modo é possível serem mais casos abrangidos pela norma e maior será a capacidade de haver uma proteção e previsão de casos concretos numa matéria tão volátil como é a proteção de dados e as tecnologias. Não há um ritmo ponderado e previsível quando falamos em tecnologias que permita ao legislador conseguir prever e acompanhar essa evolução e, por este motivo, quanto mais amplo for o conceito melhor se consegue combater este fator⁴⁰. Tendo um conhecimento completo sobre os elementos que compõe o conceito torna-se mais facilitada a tarefa de compreender o âmbito do conceito e aplicar do melhor modo possível aquilo que pretende abranger na realidade.

2.1.1. Informações relevantes

Todas as informações são consideradas como relevantes para a aplicação do Regulamento Geral de Proteção de Dados⁴¹ desde que se revelem capazes de se associarem a uma determinada pessoa, de identificá-la e fazer concluir que aquela informação é sobre aquela pessoa em específico. É esta a conclusão que se pode retirar da letra da norma quando interpretamos o conceito presente no artigo 4.º do RGPD, não existindo, deste modo, uma lista

⁴⁰ Tem sido defendida esta ideia em alguns acórdãos como o Acórdão Nowak ou o Acórdão Google Spain.

⁴¹ CORDEIRO, A. Barreto Menezes, - Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, Coimbra, Almedina, 2021, páginas 81 e ss.

taxativa do âmbito de informação relevante para que possamos aplicar o regime jurídico de proteção de dados pessoais. Uma vez mais estamos perante um âmbito abstrato que permite que não havendo motivação legal para a exclusão de uma determinada informação, possa ser considerado como dado pessoal qualquer informação, privada, profissional ou social, com “características identificadoras” de uma determinada pessoa⁴²⁴³. Cabe ainda no conceito objetos se houver uma referência e ligação entre o objeto e a pessoa a quem pertence esse mesmo objeto e seja possível fazer através dela uma interconexão entre o objeto e a pessoa a quem este pertence. Não é humanamente possível ao legislador conseguir determinar todas as informações ou tipos de informação que tenham no seu conteúdo um determinado dado pessoal e nesse sentido a limitação que seria imposta caso houvesse uma lista de informações relevantes taxativa implicaria que houvesse demasiadas situações desprotegidas legalmente. Todas as matérias são importantes para o titular dos dados e, por outro lado, seria impossível determinar o que é considerado importante para cada pessoa, o que eu considero como importante pode não ser o mesmo que outra pessoa considera e a minha consideração não deve nem pode limitar o outro. O conceito tem que ter um âmbito suficientemente amplo para abranger o mais vasto leque de casos concretos que merecem que haja uma proteção jurídica dos mesmos. A lista poderia ser, contudo, exemplificativa de modo a que pudesse haver uma linha condutora e orientadora para os aplicadores do direito, visto que sendo apenas uma lista com casos exemplo não haveria uma limitação do âmbito. O aplicador do direito ao interpretar a norma identificaria alguma das alíneas como semelhante ao caso que pretendia dar resposta e deste modo fundamentaria a sua resposta jurídica com base numa norma mais concreta.

Torna-se, contudo, essencial perceber que nem todas as informações relevantes consideradas como dados pessoais podem ser interpretadas como inacessíveis por parte da Administração Pública, não sendo a sua caracterização como dado pessoal um limitador à ação por direito da Administração Pública. Quando estamos perante um documento que é composto por nome e morada de uma determinada pessoa não podemos deduzir de modo imediato que apenas com o consentimento do titular podem ser acedidas, nem todos os dados pessoais são acessíveis apenas com o consentimento do respetivo titular. Para que possamos ter um documento que seja considerado como inacessível temos de estar perante um documento nominativo que, por outras palavras, significa que é um “documento que contenha dados

⁴² MAGALHÃES, Filipa Matias, e PEREIRA, Maria Leitão – *Regulamento Geral de Proteção de Dados - Manual Prático*, Porto, VidaEconómica, 2017.

⁴³ CORDEIRO, A. Barreto Menezes, “Direito de Proteção de Dados”, Almedina, Coimbra, 2022.

personais, na aceção do regime jurídico de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”⁴⁴. Caso não seja um documento nominativo, pode a Administração Pública aceder ao mesmo sempre que considerar necessário⁴⁵ e sem que com isso esteja a incorrer num desrespeito pelos direitos reconhecidos ao titular dos dados nos artigos 15.º e ss do RGPD. Um terceiro que queira aceder a um documento que seja considerado como nominativo só o poderá fazer caso haja uma autorização explícita e escrita do titular dos dados e desde que estejam discriminadas todas as finalidades que se pretendem atingir com o acesso que está a ser autorizado. O acesso a dados para finalidade que não esteja autorizada é uma violação de dados pessoais e deve ser restringida e consequências jurídicas poderão de ser tomadas, nomeadamente pelo incumprimento da alínea a) do n.º 1 do artigo 6.º do RGPD, que como se sabe tem aplicação direta no ordenamento jurídico português. Consagra esta alínea que quando “a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;” estamos perante um dos fundamentos de licitude⁴⁶. O acesso da Administração Pública, pelo papel que ocupa na sociedade, é apenas uma exceção à regra de necessidade de consentimento do titular dos dados.

A qualificação de uma informação como relevante e consequentemente como um dado pessoal é deste modo mais complexo do que poderia à partida parecer dado que o seu leque de abrangência é de mais difícil delimitação do que esperado numa primeira leitura e nesse sentido é necessário recorrer a outros critérios que estabelecem outros parâmetros do que pode ser definido e identificado como dado pessoal.

2.1.2. Relativa a

Quando há a menção à expressão “relativa a” estamos a tentar perceber a origem dos dados, para que objetivo foram pedidos e consentidos os dados partilhados pelo titular dos mesmos ao responsável pelo tratamento. Sempre que é requerido determinado dado é necessário que esteja delimitado o objetivo segundo os quais os dados serão utilizados, de modo a que haja um controlo e conhecimento do mapa da partilha de dados e uma maior organização do caminho que os dados percorrerão em caso de um incidente ocorrer. Quando nos dirigimos a um determinado serviço público, como por exemplo para fazer a renovação do cartão de cidadão, os

⁴⁴ Artigo 3.º n.º 1 alínea b) da Lei n.º 26/2016, de 22 de agosto.

⁴⁵ Acórdão com o processo n.º 0169/10 de 12 de maio de 2010 do Supremo Tribunal Administrativo.

⁴⁶ Acórdão com o processo n.º 0684/21.6BELSB de 3 de novembro de 2022 do Supremo Tribunal Administrativo.

dados que são recolhidos cumprem a necessidade concreta de criação do mesmo, apenas são pedidos os dados que compõe o cartão de cidadão e apenas com o objetivo de o criar. Todos os dados que sejam pedidos que não se encontrem previstos no cartão de cidadão já não estão no âmbito da finalidade a que se destina o mesmo e encontra-se em incumprimento de uma norma legal, do RGPD e do conceito por ele consagrado. O cumprimento estrito da finalidade/do objetivo estabelecido no registo de tratamento de dados é um elemento que assume um papel central da determinação e contenção da extensão de alguma partilha que possa ocorrer.

2.1.3. Pessoa identificada ou identificável

No tratamento de dados pessoais mais importante do que a determinação do conceito de informações relevantes e de quais são as finalidades consentidas pelo titular dos dados, sem descorar a sua importância, é perceber quem é o titular dos dados, ou melhor, quem pode ser o titular dos dados. Não importa perceber qual ou quais as finalidades consentidas ou que informações pessoais são relevantes sem se perceber quando temos um titular dessas mesmas informações que consentiu para que estas fossem partilhadas para uma ou mais finalidades e quando não temos, no primeiro caso merece tratamento de dados de acordo com a lei e no segundo caso não há para o responsável pelo tratamento qualquer responsabilidade.

O conceito é claro neste ponto ao afirmar que o titular dos dados tem de ser uma pessoa que possa ser identificada através daquele(s) dado(s) ou identificável quando não permite identificar de modo direto o titular dos dados, mas através dele é possível identificá-lo devido a uma correlação com outro dado ou elemento social, a ligação do dado a uma pessoa concreta tem que existir sempre. Estamos perante dados pessoais nos dois casos, contudo, não com a mesma capacidade identificativa, e o responsável pelo tratamento tem a mesma responsabilidade em ambos, não fazendo a lei qualquer distinção. A identificação do titular através de meios eletrónicos é o mais recorrente com a utilização diária de diversas fontes de dados pessoais tais como as redes sociais, a obtenção de um determinado serviço ou a marcação e realização de serviços de modo digital. Esta forma de identificação tem os seus riscos, inegavelmente, ao ser de acesso mais facilitado a quem tenha intenções reprováveis, mas também tem as suas vantagens⁴⁷ ao permitir que se tenha um acesso de modo menos moroso ao exercício dos nossos direitos e interesses. Não é o único meio ou forma, bastando recordar que sempre que nos dirigimos a um determinado local para a prestação de um serviço ou

⁴⁷ SANTOS, Sofia Berberan, e GABRIEL, João, “Regulamento Geral sobre a Proteção de Dados, Legislação e Algumas Notas”, Lisboa, Edição GPA Academy, 2020, páginas 31 a 38.

obtenção de um bem e nos é questionado determinado(s) dado(s) pessoal(ais) estamos a partilhar elementos identificativos. Desde que haja uma partilha de dados há uma forma de identificação do titular desses dados e cada uma representa sempre um risco e uma necessidade de tratamento para o responsável pelo tratamento que assume essa responsabilidade.

O critério base que norteia a definição de quais as informações relevantes que permitem a identificabilidade é inquestionável, contudo, por outro lado, não pode ser afirmado o mesmo quanto aos critérios que definem o que pode ser considerado como identificador de uma pessoa, mas que não o consegue fazer de modo direto, apesar de como vimos o tratamento que o responsável tem que cumprir por imposição legal ser exatamente o mesmo. Como podemos definir o modo como um determinado facto pode ser considerado como identificativo e outro não, o que pode uma determinada pessoa considerar como suficiente para identificar outra pode não considerar o mesmo. O considerando 26 da RGPD é a chave para esta enigma ao consagrar que terá de ser através de critérios objetivos que se deverá perceber quando através de uma determinada informação relevante estamos perante um dado pessoal, ou seja, é tendo por base a consideração de que quer o responsável pelo tratamento quer outra pessoa consegue sem grande dificuldade e sem demandar muito tempo determinar de que titular dos dados aquela informação relevante se associa. Não podem ser usados critérios subjetivos dado que podem levar a que haja mais do que uma interpretação e consequentemente pode existir a possibilidade de uma informação não ser considerada como identificadora e na verdade não ser ou a situação contrária.

Em conexão com o elemento identificativo temos de relacionar com a questão de saber se quando falamos em pessoas se estamos apenas a mencionar e referir as pessoas singulares ou se podemos incluir as pessoas coletivas cujos dados pessoais também teremos de salvaguardar e ter em consideração quando há o tratamento dos seus dados pessoais.

2.1.4. Pessoas singulares

Nos sucessivos entendimentos sobre a interpretação que deve ser feita dos conceitos presentes no RGPD tem sido um debate constante saber se as pessoas coletivas podem, por interpretação extensiva por analogia, ser consideradas como incluídas no conceito de dados pessoais, havendo quem argumente em favor e quem seja da opinião de que isso não faz sentido. Os argumentos a favor chegam à conclusão, com base em vários estudos e investigações, de que as pessoas coletivas não podem ser consideradas como titulares dos dados pessoais, não

se lhes aplicando o RGPD, visto que não se pode considerar que determinada informação relevante permite que haja a identificação de um titular dos dados em concreto. Os considerandos 1 e 2 preveem que o tratamento dos dados pessoais é um direito fundamental das pessoas singulares e que os princípios e as regras se aplicam às pessoas singulares e apenas a estas devido à sua natureza intrinsecamente pessoal⁴⁸, demonstrando deste modo que apesar dos argumentos que possam ser invocados, a lei demonstra que o âmbito da lei é apenas relativamente a pessoas singulares, descartando a possibilidade de uma interpretação extensiva segundo esta forma de pensar.

As pessoas coletivas não integram o âmbito por não haver um elemento identificativo que as identifique e distinga como tal, ao contrário do que acontece com as pessoas singulares que através do nome, por exemplo, se consegue identificar e distinguir uma pessoa de outra. A firma, apesar de identificar uma pessoa coletiva, é apenas um elemento que identifica a empresa como um todo e não uma pessoa em específico. Tem-se notado uma maior abertura a abrangência de pessoas coletivas em determinados assuntos e de serem consideradas pessoas jurídicas para o mundo jurídico, contudo, nesta matéria ainda não pode ser considerado como passível de modificação como demonstra o Regulamento Geral sobre a Proteção de Dados nos vários considerandos e artigos presentes neste diploma. Para além dos considerandos invocados, temos ainda o considerando 14 que não poderia ser mais claro quanto à exclusão das pessoas coletivas do âmbito do RGPD ao consagrar que “A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.”. Em termos de artigos⁴⁹ são vários os que demonstram que apenas se aplicam a pessoas singulares, dos quais podemos destacar, o artigo 4.º na definição prevista de dados pessoais, sendo que não podemos argumentar de outro modo e negar o que o conceito consagra e prevê.

Fica deste modo demonstrado como deve ser entendido o conceito de dados pessoais nos casos mais simples e sem grandes problemáticas doutrinárias e jurisprudenciais. Contudo como para toda a regra há uma exceção, para toda interpretação de conceitos há um conjunto de

⁴⁸ O regulamento pode ser consultado em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

⁴⁹ O artigo 1.º, 24.º, 25.º do RGPD entre outros são exemplos do que foi referido.

casos que não são de fácil e direta resolução e que implicam que sejam repensados alguns entendimentos de modo a que se possa ser mais abrangente.

2.1.5. Casos problemáticos

A aplicação do conceito presente no artigo 4.º do RGPD é na generalidade dos casos de aplicação e interpretação não problemática visto que o seu âmbito é perceptível e os critérios que norteiam o aplicador do direito, como vimos anteriormente, desde que sejam objetivos são de fácil compreensão. Há a questão abordada das pessoas coletivas, mas esta, como se demonstrou, é respondida de forma facilitada através de demonstração legal de que não é uma questão por resolver ou de equação. Nem todos os casos/situações são de fácil resolução e resposta e nesse sentido a lei não consegue responder tão de forma clara e direta às questões concretas que se podem levantar.

Um caso problemático é relativamente à consideração dos nascituros como titulares de dados relativamente a alguma partilha ou utilização dos seus dados durante a gravidez da sua progenitora. As informações que são relativas aos nascituros são dados pessoais, ao preencherem todos os requisitos do conceito de dados pessoais, tendo por isso que ser protegidos, mas não é clara a lei quanto ao facto de que os nascituros, não tendo ainda personalidade jurídica, não podem à partida assumir nenhum direito ou dever⁵⁰. Até este ponto não há dúvidas. A questão que se coloca é quem é o titular desses mesmos dados pessoais até ao momento em que o nascituro adquire a personalidade jurídica com o seu nascimento. Não há um consenso se é a mãe ou o próprio nascituro, quando adquire a personalidade jurídica, contudo é certo que os dados têm de ser protegidos e tratados, sem qualquer dúvida sobre isso, porque são dados pessoais⁵¹ ou o que ocorre quando não adquire personalidade jurídica, mas existem dados clínicos que tem dados sobre o nascituro. No caso de o nascituro não chegar a adquirir personalidade jurídica, por ter nascido sem vida, não pode ser recusado o exercício do direito de acesso à mãe relativamente aos documentos que estejam na posse do hospital sobre o parto, tempo de internamento e dados clínicos sobre o bebé nado morto ou outro documento relativo à mãe⁵². Não considerar a mãe como legítima para o acesso aos documentos descarta qualquer outro terceiro que pudesse invocar ter legitimidade para consultar, dado que, se quem

⁵⁰ O nosso Código Civil (CC) consagra que “A personalidade adquire-se no momento do nascimento completo e com vida.”, segundo o n.º 1 do artigo 66.º do CC, e que “Os direitos que a lei reconhece aos nascituros dependem do seu nascimento.”, segundo o n.º 2 do mesmo artigo. Perante este artigo reconhece-se no artigo seguinte a capacidade jurídica, que supõe a existência de personalidade jurídica para existir, e que juntos demonstram que o nascituro não tem personalidade e capacidade jurídica.

⁵¹ CORDEIRO, A. Barreto Menezes - Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, op.cit., página 114.

⁵² Parecer n.º 8/97 Data: 1997.01.16 Processo n.º 164.

gerou o feto não teve, muito menos se justifica que outros possam aceder ao mesmo. Os pais assumem deveres quando decidem prosseguir com a gravidez e passam a ser legalmente responsáveis pelo bem-estar do bebé e pela sua proteção, não se conseguindo justificar porque não o poderão ser relativamente aos dados pessoais.

Outro caso é relativamente às pessoas falecidas e à existência de uma obrigatoriedade de os seus dados pessoais continuarem a ser protegidos. Não há uma previsão no RGPD, nem nos seus artigos nem nos considerandos, sobre como deve ser regulada esta matéria sobre o tratamento de dados pessoais das pessoas falecidas⁵³, contudo, o considerando 27 2ª parte consagra que os Estados-Membros, se assim o entenderem podem regular esta matéria nos termos que considerarem relevantes e adequados. Há, deste modo, o reconhecimento que esta matéria, apesar de não prevista, não implica que não possa ser regulada pelos Estados de acordo com o que legislativamente vem de encontro à sua doutrina e jurisprudência. Os Estados-Membros aplicam a legislação europeia e cumprem-na na aplicação do direito, mas ao mesmo tempo preservam a sua soberania na tomada de decisões e posições legislativas que lhes permite aplicar normas e criar outras de uma forma coerente com aquilo que é o seu entendimento do melhor para a regularização dos seus cidadãos. No nosso país há a previsão desta matéria no artigo 17.º da Lei da Proteção de Dados Pessoais, Lei n.º 58/2019, de 8 de agosto, que consagra que apenas os dados que se inserem na denominada categoria especial⁵⁴ e os dados que se relacionam com a “à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo.”⁵⁵ é que podem ser considerados como dados das pessoas falecidas que devem ser protegidos legalmente pela lei mencionada. Contudo, não podemos deixar de constatar que o artigo 17.º é incompleto relativamente à consagração de alguns direitos, como o direito à personalidade e do que se entende ser o conceito de intimidade da vida privada e dados relativos às comunicações, tornando a especificidade nacional face ao regulamento europeu com lacunas que podem comprometer o que se entendeu necessário regular na realidade portuguesa. A pessoa designada pelo titular dos dados ou os herdeiros, caso não haja nenhuma pessoa designada,

⁵³ O artigo 68.º do CC consagra o termo da personalidade jurídica. A morte define o fim da personalidade jurídica e de todos os direitos e deveres e consequentemente subentende-se que com o termo da personalidade jurídica não existe mais o dever de tutela e tratamento dos dados pessoais da pessoa falecida.

⁵⁴ Que se encontram consagrados no artigo 9.º n.º 1 do RGPD “1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos

para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.”.

⁵⁵ Lei disponível em https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3118&tabela=leis&nversao=.

são os representantes da pessoa falecida no exercício dos direitos caso entenda que os mesmos podem não estar a ser respeitados como deveriam ou caso entenda que o prazo de conservação já foi ultrapassado.

Em termos de arquivo e tratamento de dados os serviços públicos têm um conjunto de deveres a cumprir de modo a permitir que o direito de acesso, artigo 15.º do RGPD, possa a todo o momento ser exercido na sua plenitude⁵⁶. Qualquer titular de dados pode requerer junto do serviço público o acesso aos dados que partilhou de modo a saber que dados seus foram recolhidos e para que possa exercer um dos restantes direitos se assim o entender. Os nascituros e as pessoas falecidas não são, mais uma vez, considerados neste âmbito por se entender no considerando 158 do RGPD que não podemos afirmar que as pessoas falecidas têm o direito de acesso mesmo que exercido por um representante assim como os restantes direitos. Mais uma vez se reitera que o RGPD reconhece aos Estados soberania para a determinação desta matéria e nesse sentido se um Estado entender que deve regular, dentro de determinados limites, esta matéria então poderá o fazer⁵⁷, contudo, apenas relativamente às pessoas falecidas.

Pode ser incluído neste grupo de casos problemáticos, mas que ao mesmo tempo se afasta do que pode ser considerado como verdadeiramente questionável, como é o caso dos dois exemplos mencionados anteriormente, os dados que se referem a objetos, que teoricamente não seriam considerados como dados pessoais, mas que ao se encontrarem conexos com outros dados, referentes a pessoas singulares identificadas ou identificáveis, podem ser considerados como dados pessoais. Se um determinado objeto tiver dados pessoais, como por exemplo uma etiqueta de identificação, é possível determinar e identificar a pessoa a quem pertence e consequentemente, ainda que não de modo “autónomo”, significa que terá ser tratado como todos os outros dados pessoais. Caso o objeto permita identificar a pessoa e seja posteriormente perdido ou furtado por outrem há uma partilha indevida dos dados que estejam presentes no mesmo e uma violação desses dados.

2.2. Tratamento dos Dados Pessoais

O tratamento de dados pessoais surge como preocupação a ter quando se identifica os dados partilhados e na posse de pessoa diferente do titular e que obriga a que sejam definidas normas

⁵⁶ O considerando 158 do RGPD.

⁵⁷ O Parecer n.º 277/2022 com o Processo n.º 360/2022 demonstra um caso de imposição de acesso a documentos nominativos por parte de uma herdeira relativamente aos documentos dos pais num determinado hospital e demonstra que apesar do RGPD e da recusa por parte do hospital, a nossa lei sobre a proteção dos dados nos seus artigos 17.º da Lei n.º 58/2019 de 8 de agosto e o 2133.º do Código Civil consagram que não havendo declaração em contrário por parte da(s) pessoa(s) falecida(s) não pode ser negado o acesso a documentos administrativos.

e medidas que se vão moldando à mudança que vai ocorrendo quer relativamente à quantidade de dados partilhados, quer à introdução de novos meios tecnológicos ou quer relativamente à modificação da visão que se tem sobre a vida prática e que obriga a que se mude o modo como vemos determinado caso. A cada partilha de dados que é feita num determinado serviço público ou na aquisição de um bem em concreto, é estabelecida uma obrigação para o responsável pelo tratamento que recebe esses dados e se vê deste modo obrigado, através de uma ou mais operações, a atuar para que a existência de incidentes⁵⁸ seja praticamente nula⁵⁹. Através do artigo 4.º, 2)º do RGPD é possível perceber que este mesmo objetivo pode ser concretizado através de vários meios, sejam eles automatizados ou não, e que o tratamento de dados é mais complexo do que poderia ser expectável e está presente em mais atos e momentos do que o simples momento de prestação de um serviço ou aquisição de um bem.

Os dados pessoais quando são partilhados são-no de acordo com um determinado fundamento legal que permite que a partilha tenha sido feita com respeito à legislação aplicável e não à revelia do responsável pelo tratamento que considera apenas que pode recolher os dados sem critério. Os diversos fundamentos que existem em matéria de tratamento de dados encontram-se previstos no artigo 6.º do RGPD e tem que ser tidos em consideração sempre que há uma recolha de dados pessoais. Sem um fundamento de licitude válido não pode ocorrer o tratamento dos dados e nesse sentido a recolha dos mesmos constitui uma ilegalidade praticada pelo responsável pelo tratamento. O tratamento de dados só existe se e apenas se houver um fundamento para que haja a recolha daqueles dados pessoais, tendo que ser avaliado cada caso em concreto de modo a que haja a adequação. Os fundamentos de licitude não são todos de aplicação direta e sem uma fundamentação que justifique e nesse sentido cabe ao responsável pelo tratamento fazer a ponderação e perceber qual o melhor fundamento.

A atuação de um responsável pelo tratamento tem de ser sempre tendo em consideração o que poderá ocorrer, quais as consequências negativas para o titular dos dados que se poderão concretizar, como é que futuramente o tratamento de um determinado dado de um titular se refletirá na prática. O tratamento dos dados pessoais tem de ser o objetivo principal de quem

⁵⁸ Um incidente ocorre sempre que há uma partilha indevida de dados pessoais, sempre que o titular dos dados não tiver consentido com a partilha dos mesmos.

⁵⁹ Um responsável pelo tratamento nunca pode garantir que os riscos que existem nesta matéria não existem e que os dados que lhe são partilhados se encontram salvaguardados.

⁶⁰ Consagra “«Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;”.

assume o papel de responsável pelos mesmos e deve ser definido os seus termos e o modo como vai ser estruturado esse tratamento desde o momento em que os dados são recolhidos até ao momento em que os dados são eliminados. O RGPD tem como objetivo uma proteção cada vez mais reforçada dos direitos dos titulares dos dados e nesse sentido vai designar que cada Estado-Membro tem que assumir a responsabilidade do modo como os dados estão a ser tratados e se os seus cidadãos conseguem exercer os seus direitos de uma forma direta e eficaz conseguida através da assunção pela Administração Pública, e não entidade independente como ocorria anteriormente, da análise de cada tratamento de dados de modo a que possa corrigir e impor como o tratamento deve ocorrer. Há assim deste modo uma maior proximidade entre o titular e quem efetivamente é responsável pelos dados do mesmo e a possibilidade de haver um melhor e mais rápido exercício de direitos através de uma identificação mais clara do responsável pelos dados⁶¹. Cada serviço público tem competência para exercer os direitos dos titulares dos dados sempre que entender e de compreender a quem tem que pedir justificações quando os seus direitos acabam lesados.

2.2.1. Consentimento

Um dos fundamentos de licitude que merece destaque pela sua maior dificuldade em ser aplicado na prática sem que com isso estejamos a desvalorizar um dos seus requisitos é o consentimento. O consentimento é um dos fundamentos de licitude que exige que sejam tidos em consideração as exigências da sua aplicação num determinado caso concreto para que possa ser visto a recolha dos dados pessoais como lícita. Nem todos os tratamentos que parecem poder ser baseados no consentimento o podem ser na verdade, visto que, apesar de numa primeira análise pareça ser um consentimento dado de forma livre, transparece a ideia que o titular partilhou os dados por sua vontade, a verdade é que a liberdade da partilha dos dados nem sempre existe quando parece⁶². Um contrato de trabalho tem, em termos de dados pessoais, assim como outros documentos pré-contratuais, a ilusão de que é com base no consentimento que se baseia a recolha dos dados do trabalhador, contudo, a recolha de dados pelo empregador dificilmente pode ser com base no fundamento do consentimento. A relação laboral que se estabelece parte logo do princípio de que existe uma desigualdade, em que uma das partes se encontra subordinada à outra e que fará tudo aquilo que lhe for requerido pela outra parte de

⁶¹ FREITAS, Tiago Fidalgo de *et al.* (eds.) - *Direito da Proteção de Dados: perspectivas públicas e privadas*, Coimbra, Almedina, 2023.

⁶² Podemos recorrer ao artigo 7.º do RGPD que estabelece as condições do consentimento para que possa ser um fundamento de licitude, em conjunto com o artigo 6.º n.º 4 também do RGPD e das Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679. Estas diretivas são um dos instrumentos criados pela União de modo a orientar os Estados pela correta definição do que se pode entender quando falamos em consentimento.

modo a conseguir o seu objetivo pessoal, obter o emprego para o qual se está a candidatar. Assim acontece quando o Estado pede ao cidadão alguns dos seus dados pessoais para que um determinado serviço lhe possa ser prestado, o cidadão ao querer que lhe seja prestado esse serviço automaticamente partilha esses dados ou quando há a criação do cartão de cidadão não há uma opção para o cidadão em querer ou não querer que os seus dados sejam partilhados. O cidadão partilha com o Estado os seus dados, mas apenas porque sabe que precisa daquele serviço ou de ter o cartão de cidadão, parece que fornece os dados porque quer, mas não passa de aparência. O considerando 32 consagra que o consentimento tem de ser “um ato positivo 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”⁶³ não podendo ser fundamento de um tratamento que não cumpre um destes requisitos. Se há uma relação de subordinação, de hierarquia, entre o responsável pelo tratamento e o titular dos dados o consentimento nunca poderá ser totalmente livre, apesar de o trabalhador aparentemente partilhar os dados livremente. Pode ser específico, informado e inequívoco, mas não poderá ser livre. Basta pensarmos no que acontecerá caso o trabalhador se recuse a partilhar determinados dados, poderá o contrato ser celebrado e as diligências pré-contratuais serem cumpridas sem esses dados? Não há uma resposta certa a esta pergunta, mas é previsível que a resposta seja negativa. O que acontecerá se o cidadão se recusar a fornecer dados a um determinado serviço público ou a ter cartão de cidadão, conseguirá ter os seus interesses cumpridos ou aceder a determinados serviços sem que se tenha de identificar? A resposta também parece negativa. Não conseguindo e tendo de o fazer então o consentimento que parece existir, apenas forneceu o cartão de cidadão ou apenas o criou porque deu os dados de livre vontade, na verdade não existe, pelo menos não para todos os cidadãos.

O responsável pelo tratamento tem que conseguir provar e demonstrar que o consentimento dado pelo titular foi efetivamente livre, específico, informado e inequívoco de modo a que o consentimento possa ser visto como fundamento de licitude⁶⁴. Caso os dados sejam recolhidos para finalidades diferentes tem que o titular dos dados conseguir separar o seu consentimento e decidir sobre o mesmo relativamente a cada uma dessas finalidades. A vontade que norteia um consentimento tem de ser sempre relativa a uma finalidade específica, tem o titular de saber

⁶³ O artigo 4.º, 11) do RGPD consagra a definição de consentimento e vai na mesma linha do considerando ao definir o consentimento como sendo “uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”.

⁶⁴ O considerando 43 vem estabelecer as características que o consentimento tem que reunir para que estejamos perante um fundamento de tratamento lícito no âmbito do artigo 6.º.

para o que em concreto é pedido o seu consentimento, tendo de haver a especificação das diferentes finalidades, caso aplicável, existentes no caso, tem de ser informada quanto ao que se está a dar o consentimento e tem de ser inequívoca quanto ao conteúdo e finalidade do tratamento⁶⁵. A vontade específica é um mecanismo de impedir que haja outras finalidades que possam ser perseguidas pelo responsável no tratamento e que nada se relacionem com as que o titular consentiu e para as quais poderia nem concordar⁶⁶. Ter um consentimento como fundamento de licitude implica também que haja um conhecimento do titular de como poderá exercer os seus direitos sempre que entender e que tal como facilmente dá o seu consentimento, do mesmo modo deve ter ao seu dispor mecanismos criados pelo responsável pelo tratamento que permitam retirar o seu consentimento a todo o tempo⁶⁷.

O consentimento, tal como todos os aspetos que compõe o tratamento de dados pessoais, tem de respeitar e cumprir um conjunto de princípios que norteiam o tratamento de acordo com o que legalmente se consideram ser os limites básicos que tem sempre de ser tidos em consideração quando temos um tratamento de dados.

2.2.2. Princípios aplicáveis em matéria de proteção de dados

Os princípios gerais do direito constituem uma fonte jurídica que motiva, baseia e inspira todos os ramos jurídicos e servem de ponto de referência para a constituição de outros princípios mais específicos e que se adequam às necessidades de cada um dos ramos jurídicos do Direito. Norteiam a aplicabilidade das normas em matéria de proteção de dados e ajudam a perceber de que modo é que a norma interpretada pode ser aplicada no caso concreto de forma a respeitar o que o legislador quis transmitir com a norma, perspetiva subjetivista da interpretação, e que critérios objetivos, perspetiva objetivista da interpretação, estão presentes na norma. Os princípios são um meio de, por um lado, implementação de obrigações para a responsável pelo tratamento, em que impõe a proporcionalidade entre a finalidade e os dados recolhidos (princípio da proporcionalidade), e, por outro lado, um instrumento de orientação e de ponderação na aplicabilidade de medidas técnicas e organizativas que permitem que as suas funções sejam mais alinhadas com os interesses do titular e com os seus próprios interesses em tomar todas

⁶⁵ Diretrizes 05/2020 páginas 15 e 16 consagram o que deve ser entendida uma vontade específica, que exigências tem de ser cumpridas para que possamos ter uma vontade específica.

⁶⁶ A exigência de uma vontade relaciona-se com o princípio da transparência, consagrado no artigo 5.º n.º 1 alínea a) do RGPD, ao impor que para que um titular possa ter um consentimento livre tem de saber com que está a consentir, os limites desse consentimento e de que modo pode retirar o consentimento caso não concorde com o mesmo.

⁶⁷ Diretrizes 05/2020 páginas 17 e 18.

as medidas que permitam que os riscos de incidentes sejam o menor possível e a consciência de que fez tudo aquilo que a responsabilidade assumida lhe impunha.

Podemos enumerar alguns dos principais princípios em matéria de proteção de dados, sendo eles, o princípio da licitude, o princípio da lealdade, o princípio da transparência, o princípio da administração aberta, o princípio da boa administração, o princípio da limitação das finalidades, o princípio da minimização de dados, o princípio da exatidão, o princípio da limitação da conservação, o princípio da integridade e confidencialidade e o princípio da responsabilidade, encontrando-se todos consagrados no artigo 5.º do RGPD. O responsável pelo tratamento de dados pessoais tem sempre de aplicar os princípios de forma impiedosa de modo a que cumpra as normas e as suas responsabilidades legais, de forma saber como determinar como deve atuar num determinado caso que lhe surja dúvidas sobre a sua atuação ou como forma de orientar o seu comportamento como responsável de acordo com a lei e com os requisitos e exigências que desta advém e que nem sempre são de fácil compreensão e aplicação. Os princípios servem deste modo como bússolas na aplicação do direito aos casos concretos e às especificidades que cada um deles representa, dado que, o legislador não tem a capacidade, por ser impossível ter, de determinar todos os casos concretos e as suas especificidades. Nenhum caso concreto é igual ao outro, nenhum legislador consegue prever todos os casos nem consegue transmitir na sua plenitude o pensamento jurídico que motivou aquela norma, cabendo a quem aplica a norma a interpretação da mesma. Todos os princípios que se aplicam em matéria de proteção de dados, para além do que já foi referido quanto ao responsável, visam a proteção da intimidade e da vida privada dos titulares dos dados pessoais se tenha em consideração e que seja a prioridade e atuam como protetores destes direitos dos titulares, assim como noutras matérias, não tendo outra finalidade.

Jurisprudencialmente são invocados os princípios como fundamento de decisão sobre que resposta jurídica deve ser dada a um determinado caso concreto onde o responsável pelo tratamento dos dados não cumpriu com os pressupostos ou caso o tenha feito não se revelou suficiente para que o incidente não ocorresse⁶⁸. É com base nos princípios, e outros elementos, que vai permitir que haja uma ponderação de todos os elementos de prova existentes e a determinação de que forma deve ser interpretada e analisada a responsabilidade do responsável pelo tratamento num determinado caso concreto. Caso haja uma ponderação indicadora de que

⁶⁸ Podemos para este efeito consultar o acórdão do Tribunal da Relação de Lisboa disponível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f29bb6d27dadeeb28025819c00508fe8?OpenDocument>.

apesar do cumprimento das normas e do tratamento dos dados apenas de acordo com as finalidades o incidente ocorreu estaremos a falar de uma responsabilidade, que existe sempre, do responsável pelo tratamento diferente face àquela que existiria caso não tivesse havido esse cumprimento.

O tema desta dissertação impõe que seja dado relevo a dois dos princípios é o princípio da lealdade e o princípio da segurança, revelando-se imperiosos na determinação da responsabilidade em caso de incidentes. A escolha por estes dois princípios tem como fundamento a sua importância para a delimitação da responsabilidade dos responsáveis pelo tratamento. Estes têm um papel central na proteção dos dados pessoais que lhes são confiados. Nesse sentido a sua atuação deve ser sempre de acordo com a ideia de que a proteção que lhes é confiada não pode ser outra senão aquela que permita ao titular dos dados conhecer a todo o momento que tratamento de dados que está a ser feito, e não apenas no início quando partilha os dados, e por outro lado esse tratamento tem que ser feito no interesse de uma proteção adequada e conforme as medidas técnicas e organizativas que se justifiquem face aos dados partilhados e responsabilidade assumida pelo responsável pelo tratamento. A responsabilidade que vai ser abordada no ponto 3. deriva e tem efeito naquilo que o responsável faz ao longo da sua atuação, desde o momento em que o titular partilha os dados até ao momento em que o tratamento deixa de existir. Os outros princípios são relevantes no tratamento de dados pessoais, mas para questões de responsabilidade assumida em caso de tratamento ou partilha indevida de dados, são estes os princípios fundamentais, se o titular foi informado e se as medidas adequadas foram adotadas.

2.2.2.1. Princípio da Lealdade

O princípio da lealdade encontra-se consagrado na alínea a) do n.º 1 do artigo 5.º do RGPD em conjunto com outros dois princípios que em conjunto com aquele impõe nos primeiros momentos determinados requisitos para que o tratamento de dados possa ocorrer de acordo sempre com a imperatriz do tratamento de dados pessoais, ou seja, tendo sempre em consideração os direitos e os interesses do titular dos dados. Estamos a falar do princípio da transparência e o princípio da licitude como dois princípios que em conjunto com o princípio da lealdade norteiam o responsável pelo tratamento e lhe impõe os limites e exigências em matéria de proteção de dados.

O princípio da lealdade relaciona-se com a exigência de que o titular dos dados tem de estar sempre informado sobre a partilha dos dados que consentiu e confiou ao responsável pelo titular dos dados. O titular dos dados só consente livremente, um dos requisitos essenciais do consentimento, caso tenha sido informado da(s) finalidade(s) do tratamento na sua íntegra e perceba o que estas representam em termos de partilha dos seus dados pessoais. Sem o conhecimento de todos os aspetos do tratamento dos dados nunca poderá o consentimento ser verdadeiramente livre dado que o titular não consentiu sobre um ou mais aspetos⁶⁹. Um titular que não tenha a intenção de partilhar os seus dados para uma finalidade que não tenha sido transmitida não pode dar o seu consentimento para tal. Quando ocorreu a partilha dos dados esta ocorre porque o titular assim o quis e não apenas porque poderia estar subentendido pelo responsável pelo tratamento de que apenas lhe bastava ter em conta os interesses do titular para que o cumprimento de lei estivesse a ser praticado e o consentimento fosse fundamento de licitude. Os artigos 13.º e 14.º preveem que o cumprimento por parte do responsável pelo tratamento deste conjunto de obrigações sobre as informações que devem sempre ser prestadas ao titular dos dados de modo a cumprir o princípio da lealdade e a possibilitar que os casos que se baseiam no consentimento o possam ser. O responsável pelo tratamento não pode nunca descorar as suas obrigações e deixar de atuar em conformidade com a lei, interesses e direitos do titular e desvalorizar o seu papel no cumprimento das mesmas, não podendo assumir que se o titular consentiu ele saberia dos riscos que a partilha dos dados representa.

Como foi mencionado anteriormente este princípio encontra-se em correlação com outros dois que tem de ser e são cumpridos de modo a que possamos ter o cumprimento do princípio da lealdade. Os três princípios relacionam-se e interligam-se entre si. Um dos princípios, tal como foi mencionado, é o princípio da transparência que consagra que o tratamento dos dados tem de ser baseado na clareza das finalidades do tratamento e de todos os atos praticados pelo responsável. Não podem haver atos dos quais o titular não tenha entendido na sua plenitude e não podem haver falta de honestidade por parte do responsável quando está a prestar as informações de acordo com o imposto nos mencionados artigos 13.º e 14.º do RGPD. Só com esta explicação breve sobre o que se entende pelo princípio já é perceptível a sua correlação com o princípio da lealdade, dado que, só podemos ter um consentimento livre se este for informado sobre tudo aquilo que recai e o for de forma transparente e esclarecedor para o titular dos dados.

⁶⁹ MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais*, op.cit., página 102.

O outro princípio, por sua vez, é o princípio da licitude que estabelece que o tratamento tem de ser de acordo com as disposições legais que impõe os requisitos a obedecer por parte do responsável de modo a que possamos ter um tratamento leal e transparente dos nossos dados pessoais e tenhamos deste modo um consentimento que possa ser considerado como livre e fundamento desse mesmo tratamento. Encontram-se deste modo conexos os três princípios como um só e como suporte uns dos outros para a sua aplicabilidade como um todo e como impulsionadores para que os dados pessoais dos titulares sejam sempre vistos pelo responsável pela importância que representam.

Recai sobre o responsável pelo tratamento a responsabilidade pelo cumprimento deste princípio de forma sublime e na sua íntegra em todos os momentos da “sua responsabilidade” e em todos os atos que praticar relativamente ou com os dados do titular dos dados. O cumprimento deste princípio tem de ser conseguido através da criação e previsão de meios suficientes e claros para que possa o titular, sempre que entender, exercer os seus direitos. O titular tem de ter sempre, como forma de exercício dos seus direitos, mecanismos de exercício de direitos que lhe permitam exercê-los sempre que considerar que algum dos seus direitos ou interesses não está a ser cumprido. O responsável tem de informar sempre com clareza, transparência, de forma informada e de acordo com as disposições legais esses mesmos mecanismos ao titular dos dados sempre que este consente com a sua partilha. Não podem haver questões sobre os mecanismos ou até mesmo desconhecimento sobre a sua existência sendo o exercício dos direitos pelo titular dos dados uma das obrigações do responsável pelo tratamento. Ocorrendo uma desconformidade no tratamento o titular tem de saber sempre quais os mecanismos que pode recorrer, como o pode fazer e que respostas e respetivos fundamentos poderá ter ao uso dos mesmos. Tem de ser criados sempre com vista o melhor exercício dos direitos e interesses do titular, para além do óbvio cumprimento legal. Não adianta ter os meios previstos se o titular não tiver forma de perceber de forma indúbia do que consistem esses meios e como pode beneficiar dos mesmos.

A Administração Pública quando atua como responsável pelo tratamento dos dados dos seus cidadãos tem de o fazer com a consciência de que, apesar de a lei não fazer uma diferenciação entre responsáveis pelo tratamento, assume uma responsabilidade que se diferencia para o titular dos dados. Não há uma discriminação legal, mas a verdade é que uma partilha de dados numa entidade privada não tem as mesmas consequências, quer pelo possível

número de dados partilhados quer pela importância que o responsável assume perante um cidadão, que aquela que existem caso ocorra num determinado serviço público. Há uma imposição mais exigente do modo como é o comportamento do Estado como responsável pelo tratamento que se justifica e leva a que a transparência do seu comportamento deva ser cumprida de forma eximia. Se há elementos pouco esclarecedores no tratamento é necessário corrigir⁷⁰, a Administração Pública tem de ser proativa e atuar sempre antes dos problemas, antes das limitações de exercícios dos direitos e antes de qualquer argumento negativo ou demonstrador de que se tivesse atuado de outro modo os riscos de partilha ou modificação ou desaparecimento indevida poderiam ter sido evitados, fazendo-o sempre com o conhecimento de que é seu dever informar os cidadãos⁷¹. O princípio da administração aberta não poderia ser melhor impulsionador da necessidade de transparência que tem que existir no tratamento de dados pessoais pela Administração Pública e de que forma a proatividade que deve existir pode beneficiar com a possibilidade de os titulares terem sempre acesso de forma clara aos seus dados pessoais.

2.2.2.2. Princípio da Segurança

Um outro princípio nesta matéria é o princípio da segurança⁷², princípio este que se encontra relacionado com o princípio da confidencialidade e encontra-se previsto na alínea f) do n.º 1 do artigo 5.º do RPDG, que consagra a imposição da obrigação ao responsável pelo tratamento de que o tratamento dos dados por si efetuado seja sempre de acordo com as normas da segurança dos dados, independentemente das circunstâncias. As medidas técnicas e organizativas adotadas têm de ser sempre criadas tendo em consideração os dados aos quais se vão aplicar, à sua relevância e ao seu formato de conservação de modo a que haja uma adaptação do comportamento do responsável pelo tratamento aos diferentes riscos que podem existir⁷³. O responsável deve estruturar antes de recolher os dados o modo como o tratamento dos mesmos irá ocorrer, como será a sua conservação e que medidas serão adotadas para o caso de haver a partilha indevida dos dados. Este planeamento não deve ocorrer num momento posterior e deve, por outro lado, ser adaptado caso se revele insuficiente ao circunstancialismo que foi tido em consideração mas que se revelou insuficiente na prática ou caso tenha-se alterado algum

⁷⁰ FREITAS, Tiago Fidalgo, e ALVES, Pedro Delgado – *O acesso à informação administrativa*, 1ª Edição, Almedina, 2021.

⁷¹ Prevê o artigo 11.º do Código do Procedimento Administrativo no seu n.º 1 “Os órgãos da Administração Pública devem atuar em estreita colaboração com os particulares, cumprindo-lhes, designadamente, prestar aos particulares as informações e os esclarecimentos de que careçam”.

⁷² Encontra-se previsto no artigo 5.º n.º 1 alínea e) do RPDG e onde é consagrado o ónus imposto aos responsáveis pelo tratamento de dados pessoais.

⁷³ SALDANHA, Nuno – *Novo Regulamento Geral de Proteção de Dados - O que é? A quem se aplica? Como implementar?*, Lisboa, FCA, 2020.

ponto de ponderação no tratamento adequado e que leva a que se modifique o mesmo sob pena de se revelar desadequado e incumpridor de normas⁷⁴. Todos os dados são, a partir do momento em que o titular os partilha, confidenciais e íntegros não relevando nenhuma circunstância como argumento justificativo para a ocorrência da partilha indevida ou para que estes sejam modificados, esquecidos ou perdidos sem que haja consentimento ou conhecimento do titular dos dados. O não cumprimento deste princípio representa uma contraordenação grave devendo sempre que possível recorrer à anonimização⁷⁵ ou à pseudonimização⁷⁶ dos dados que identifiquem o titular dos dados de modo a reforçar a segurança e a confidencialidade dos mesmos⁷⁷.

Este princípio não se encontrava consagrado na Diretiva 95/46/CE e resulta de uma sugestão e proposta do Parlamento de modo a diminuir os riscos da partilha dos dados ao atribuir mais responsabilidade ao responsável pelo tratamento. Foi visto como um princípio que era a peça que faltava no puzzle dos princípios e que iria contribuir para que a evolução que se estava a registar na digitalização e na quantidade de dados partilhados que estava a existir, muitas vezes irrefletida como vimos, fosse mais cautelosa e, por outro lado, adequada a essas mesmas circunstâncias. Ao impor que os dados sejam tratados como confidenciais, independentemente do que possa ser o seu circunstancialismo, e que cabe ao responsável garantir que existam meios de reforço da sua responsabilidade para proteção dos dados pessoais que passa a ser responsável, permite que a evolução possa ocorrer e que estejamos perante de uma realidade com regras. Este princípio foi ainda pensado para se aplicar aos subcontratantes que assumam em nome do responsável pelo tratamento o tratamento de determinados dados recolhidos pelo responsável e que devem-se comportar, como veremos, da mesma maneira que o responsável e segundo as orientações que lhe são dadas por este. O responsável assume sempre a responsabilidade pelos atos praticados pelo subcontratante e, nesse sentido, deve garantir que

⁷⁴ SANTOS, Graça - *O Regulamento Geral de Proteção de Dados da Teoria à Prática*, Lisboa, Chiado Editorial, 2023.

⁷⁵ O responsável ao recorrer à anonimização divide, de forma irreversível, as informações de modo a que seja mais complicada a identificação do titular dos dados, tornando deste modo os dados mais confidenciais e consequentemente seguros, concretizando deste modo o princípio da segurança.

⁷⁶ De modo a tornar os dados mais confidenciais e cumprindo de forma sublime o princípio da segurança o responsável pode também recorrer à pseudonimização dos dados, que significa que os dados, tal como na anonimização, são separados, contudo, com a diferença de que se necessário é possível juntar de novo os dados e identificar o titular dos dados. A medida não torna deste modo os dados separados de forma irreversível.

⁷⁷ RODRIGUES, José Noronha, e TEVES, Daniela Medeiros – *A proteção de dados pessoais e a Administração Pública – O novo paradigma jurídico*, Lisboa, AAFDL Editora, 2020, página 54.

este assume as medidas técnicas e organizativas por si adotadas e que cumpre todas as normas e princípios que se impõe ao tratamento de dados pessoais⁷⁸.

2.2.3. Problemáticas do tratamento de dados pessoais

O tratamento de dados pessoais nem sempre é uma tarefa pacífica na determinação do seu âmbito de atuação e que comportamentos representam uma ameaça aos direitos e interesses que se visam salvaguardar, os do titular dos dados, e quais são as medidas que serão mais eficazes para que a tutela dos dados seja feita de acordo com a expectativa gerada.

Um dos problemas que pode surgir quando o responsável pelo tratamento inicia a sua delimitação de como os dados tem que ser tratados é o entendimento de quais são os meios e medidas técnicas e organizativas que devem ser adotadas de modo a minimizar os riscos que o tratamento representa para os interesses e direitos do titular dos dados. O responsável não consegue prever e projetar no presente, assim como acontece com o legislador, todos os momentos da sua atuação que podem significar um risco ou quais os comportamentos que terceiros, subcontratantes, que atuam em seu nome podem ser um iminente risco ou ainda que comportamentos de pessoas que em nada se relacionam com o titular ou com o responsável ou seu subcontratante, os verdadeiros terceiros. O responsável assume a obrigação de prever todos os riscos que conseguir, contudo, não pode nunca assegurar que, tal como foi mencionado antes, que em nenhum momento surgirá um desrespeito pelos dados pessoais.

O principal problema no tratamento de dados, e que foi sendo várias vezes mencionado, é a possibilidade iminente e real de haver uma partilha indevida dos dados a qualquer momento e que apesar dos esforços que sejam encabeçados pelo responsável pelo tratamento não há maneira de impedir que os mesmos ocorram. Estes podem ocorrer com um conjunto de medidas técnicas e organizativas adequadas a ser postas em prática e a serem sempre cumpridas ou no caso completamente oposto, a responsabilidade do responsável pelo tratamento existe sempre e independentemente de tudo o que foi feito para prevenir. É uma certeza de que o responsável assumirá toda a responsabilidade pelas violações de dados que ocorram sem que possa argumentar de que não teve qualquer intenção ou culpa pelo que sucedeu.

⁷⁸ Texto retirado do Eur-Lex sem autor identificado, com a data de 08/03/2014, encontrando-se disponível em <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>.

3. Violações de Dados

Os riscos com as partilhas indevidas de dados existem desde o momento em que o titular partilha os seus dados até à sua eliminação dos sistemas informáticos e backups que existem na rede de trabalho do responsável pelo tratamento, independentemente das medidas de segurança que são adotadas e seguidas, e tem que ser acautelados para que não passem da mera possibilidade para a realização na prática. A prudência que é exigida ao responsável pelo tratamento e a imposição de normas de tratamento têm que existir, mas sempre com a consciencialização dada ao titular dos dados que incidentes podem ocorrer e que meios tem estes disponíveis para reagir. O responsável tem conhecimento de que para além das normas do modo como cada dado tem que ser conservado, há que saber como deve ser a sua atuação caso um ataque informático ou algum erro por sua parte ocorrer e como pode impedir que as consequências negativas sejam de uma proporção evitável. A atuação de um responsável que tem uma organização que lhe permite conhecer o “percurso” que os dados que detêm percorrem e dos casos em que o titular tem que ser informado de forma a poder tomar precauções são essenciais para que o que ocorreu já de negativo não seja mais danoso para os titulares dos dados. Quanto maior for o número de dados que são recolhidos maior será o risco de ocorrer uma violação de dados, maior é a necessidade de que o tratamento desempenhado seja adequado e maior é a exigência de que o responsável pelo tratamento tenha a responsabilidade bem definida e organizada.

Uma violação de dados pode ser definida como “uma violação da segurança que provoque, de modo accidental 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” nos termos do artigo 4.º, 12). Representa deste modo alteração ou partilha indevida dos dados pessoais que foram partilhados pelo titular com base ou de acordo com uma ou mais finalidades específicas e de acordo com as medidas e meios de segurança que confiaram ser suficientes e que sem o seu consentimento assistem a uma violação daquilo que lhes foi prometido. O titular dos dados tinha uma expectativa jurídica de quais eram as finalidades de tratamento dos seus dados e que estes estariam salvaguardados de qualquer modificação ao seu conteúdo, mas, por atos de terceiros, acabam por verificar que quem assumiu a responsabilidade de lhes prestar um serviço ou fornecer um determinado bem não conseguiu fazê-lo sem que requerido para o fazer acabem por condicionar ou inviabilizar o que era pretendido pelo titular quando partilhou os seus dados. Se houvesse o conhecimento deste de

que os seus dados seriam partilhados de forma indiscriminada e sem qualquer controlo ou seriam modificados poderia ter tomado outra decisão quanto à ponderação entre a execução de serviços e aquisição de bens para seu interesse e a partilha dos seus dados.

A violação dos dados pode ser dividida em três tipos⁷⁹ de acordo com o que o princípio que foi posto em causa com a violação dos dados, podendo estar baseada numa partilha indevida dos dados, princípio da confidencialidade, numa alteração dos mesmos quer de forma accidental ou quer seja sem autorização, princípio da integridade, ou na perda de acesso ou sua destruição sem que tenha existido o exercício dessa vontade pelo titular⁸⁰, princípio da disponibilidade⁸¹. Esta ideia das diferentes problemáticas que podem acontecer sem o consentimento do titular dos dados demonstra que apesar da adoção de todas as medidas técnicas e organizativas os dados nem sempre estão salvaguardados ou nem sempre estão reunidas todas as condições para que todos os riscos venham mesmo a concretizar-se e que todos os tipos de violação de dados mencionados podem ocorrer em simultâneo na mesma situação. Todas estas violações de dados devem ser documentadas de modo a que o responsável tenha um registo de todos os incidentes que ocorreram, que dados foram postos afetados e quais foram as medidas adotadas posteriormente ao ocorrido para que assim tenham um mecanismo de demonstração de responsabilidade e de empenho naquilo que terão de modificar na sua atuação como responsável. Apesar de nem sempre haver um descuido e tudo aquilo que era exigível a um responsável ter sido feito, a verdade é há sempre algum ponto que poderia ser melhor trabalhado e que levou, ou não, a que a violação dos dados ocorresse. Há, para além do que foi exposto, ainda a exigência de saber como devem proceder de modo a que possam de alguma forma assumir a responsabilidade de saber atuar e dar respostas sobre o circunstancialismo da violação de dados que ocorreu.

3.1. Procedimento em caso de violação de dados

O procedimento em caso de violação de dados encontra-se definido legalmente nos artigos 33.º e 34.º e nos considerandos 85 a 88 do RGPD que nos veem orientar do que devemos entender como violação de dados e de que forma tem os responsáveis pelo tratamento de dados a obrigação de ter conhecimento sobre como devem atuar e de quais são os primeiros deveres

⁷⁹ Alínea f) do n.º 1 do artigo 5.º do RGPD.

⁸⁰ O RGPD prevê no artigo 17.º as possibilidades de os titulares dos dados requererem que os seus dados sejam destruídos a partir do momento em que o tratamento dos seus dados passar a não existir e o responsável deixar de ter fundamento de licitude para o fazer. Este direito apenas existe se o tratamento de dados não for baseado no exercício de obrigações legais. Caso seja feita sem que o titular tenha requerido ou sem que haja a imposição legal de o fazer, quando os prazos de conservação são atingidos, há uma clara violação dos dados.

⁸¹ O Grupo de Trabalho do artigo 29.º para a proteção de dados veio defender que são estes os três tipos de violações que podem ocorrer.

depois de ocorrer uma violação de dados. Há um conjunto de deveres que tem que ser postos em prática previamente e como modo preventivo do que possa ocorrer, como foi feita menção anteriormente, mas que apenas existem como meio para evitar que haja a violação de dados e podem apenas servir como posteriores atenuantes face às consequências que a violação de dados pode significar. Depois de a violação de dados ocorrer o objetivo passa a ser o de controlar os danos que dela resultaram, avaliar o que pode ter levado à violação de dados e as fragilidades que o tratamento de dados tem que devem ser corrigidas para um futuro melhor.

Num primeiro passo é necessário comunicar à autoridade de controlo, num prazo de 72 horas, de acordo com o artigo 33.º do RGPD, e aos titulares dos dados⁸² que ocorreu uma violação dos seus dados pessoais, qual a extensão e consequências da mesma e que precauções devem tomar tendo em conta os dados que tenham sido partilhados, modificados ou perdidos com o incidente. Existem vários critérios que são utilizados para orientar o modo de proceder junto do titular dos dados e nesse sentido determinar, de imediato, se os titulares dos dados têm ou não que tomar conhecimento de que os seus dados foram em parte ou num todo afetados e que dados em concreto. O dever de transmitir ao titular dos dados é excecionado pelo n.º 3 do artigo 34.º do RGPD que consagra que caso não haja motivos para crer que as medidas técnicas e organizativas não existiam ou não foram adotadas, que todos os atos necessários para proteger os direitos, liberdades e garantias foram adotados e caso implique um esforço desproporcional a comunicação individual e que esta pode ser substituída por uma informação dada a todos os titulares dos dados, cumprindo deste modo mais simples o direito à informação dos titulares dos dados, não existe a exigência de cumprir o dever de informação a cada titular e de forma individualizada. A comunicação ao titular representa sempre uma importância prioritária face à feita às autoridades de controlo, devendo ocorrer sempre que exista um “elevado risco” que provoquem “danos físicos reversíveis ou não reversíveis” para o titular⁸³, servindo a comunicação para alertar o titular dos dados da cautela que tem que assumir face a “fragilidade” dos seus dados⁸⁴. Os danos que podem existir e que põe em causa a segurança dos dados são aqueles

⁸² Obedece este dever de comunicação em todo o seu conteúdo ao princípio da segurança na medida em que a comunicação tem de ser sempre transparente com o titular dos dados e revelar na íntegra quais os dados que foram envolvidos no incidente, as consequências, as medidas adotadas e as precauções que o titular deve ter em consideração. O artigo 12.º do RGPD é claro quanto à necessidade de as comunicações com o titular dos dados terem de ser o mais transparentes possível. Não podem restar dúvidas ao titular sobre o que ocorreu no incidente e o que este significou para os seus dados.

⁸³ O RGPD fala em elevado risco, mas não define o que pode ser entendido como elevado risco e em que situações, a título de exemplo, devem ser consideradas como de elevado risco. A definição apenas foi avançada pelo Grupo de Trabalho do artigo 29.º e que situações é que estavam aqui inseridas. O legislador europeu ficou aquém nesta definição que se revela essencial para a definição dos casos em que é preciso que haja a comunicação e conduz a situações em que não se consegue definir com toda a certeza se há ou não a responsabilidade de comunicar o incidente.

⁸⁴ O titular dos dados ao tomar conhecimento que os seus dados foram partilhados indevidamente ou com quem não tinha competência fica consciente de que os seus dados poderão ser utilizados para finalidades com as quais não concorda e até ilícitas.

em que ocorreu uma violação que permitiu que houvesse um acesso aos dados por quem não tem competência, como vimos violação de dados por incumprimento do princípio da confidencialidade, ou que levou a um impedimento de acesso ou destruição dos dados, violação do princípio da disponibilidade, e são estes danos que afetam o titular dos dados e permitem afirmar que face à autoridade de controlo que vai avaliar a extensão do incidente são mais importantes os titulares dos dados. A importância da comunicação à autoridade de controlo não está aqui a ser descorada, de modo algum, pois o seu papel não se questiona, mas o papel deste é também ele pensado no titular dos dados apenas e é nesse sentido que referi que os titulares dos dados são a prioridade.

Caso o responsável não pratique os atos que são adequados ao caso e não comunique ao titular, a autoridade de controlo assumirá esse papel⁸⁵, essa obrigação, nos casos em que tem que haver essa comunicação, e comunicará ao titular dos dados. Independentemente de como ocorreu o incidente ou de quem comunica o mesmo, a verdade é que o titular tem de ser sempre a preocupação que deve e tem de ser assumida por quem tem a responsabilidade e competência para o fazer. A este possível impasse no assumir do dever de comunicação, acresce os casos em que existe um subcontratante que terá de comunicar ao responsável o incidente e adotar todas as medidas técnicas e organizativas estabelecidas pelo responsável pelo tratamento de forma a mitigar os danos, ao mesmo tempo que este toma a decisão se tem ou não de comunicar aos titulares dos dados e assume a obrigação de comunicar às autoridades de controlo no prazo de 72 horas. Como já foi expresso anteriormente o responsável assume sempre a responsabilidade pelos atos praticados pelo subcontratante desde que este tenha cumprido todas as medidas e orientações estabelecidas pelo responsável, não devendo ser a violação dos dados imputada ao subcontratante. O titular dos dados não tem interesse em saber quem trata os seus dados, mas sim que os mesmos sejam protegidos e que caso a violação dos dados ocorra o responsável assuma a responsabilidade.

Para além de sabermos quem assume a responsabilidade de comunicar ao titular dos dados em caso de violação de dados, é necessário entender quais são os procedimentos que podem ser adotados de modo a que possam os titulares dos dados reagir à violação dos seus dados pessoais e deste modo conter e prevenir-se dos efeitos negativos que podem existir. Quando ocorre uma violação de dados pessoais estamos perante um dano que é provocado na esfera

⁸⁵ N.º 4 do artigo 34.º do RGPD.

jurídica do titular desses dados, que pode ser muitas vezes irreparável ou reparável, e que tem que ser reparado. O titular dos dados tem que ter conhecimento perante quem pode reagir e como se pode defender e proteger. Quem assume a responsabilidade numa violação de dados? Quem determina como e quem responde? Que mecanismos são determinados pelo responsável pelo tratamento para que possa reagir depois da comunicação da violação de dados?

3.2. Entidades competentes na responsabilidade

Uma violação de dados implica que para além das comunicações necessárias haja uma determinação pela autoridade de controlo de quem assume a responsabilidade pelo tratamento de dados. Muitas vezes quem se apresenta perante o titular dos dados não é o responsável pelo tratamento, mas sim um subcontratante ou um sub-subcontratante que atua em seu nome e que não assume a responsabilidade pelos dados que trata e que apenas cumpre as finalidades e medidas técnicas e organizativas que o responsável pelo tratamento designa.

A necessidade de proteção e de adoção de normas de segurança como as que são criadas hoje em dia não podem ser comparadas com o que em 1995, quando se criou a Diretiva, dado que a perceção sobre os dados pessoais, sobre as necessidades que o tratamento de dados tem de ter e a responsabilidade que tem de ser assumida e respetivo âmbito mudaram drasticamente com a digitalização a assumir contornos que antes eram impensáveis. A responsabilidade assumida é mais exigente e mais complexa e consequentemente a resposta a possíveis situações de violações de dados tem de ter em consideração as alterações que nesta matéria se foram verificando e a necessidade de haver uma resposta cada vez melhor aos problemas que vão surgindo. Os riscos estão mais iminentes independentemente daquilo que é adotado dado que a quantidade de dados, a existência de instrumentos de inteligência artificial e o aumento do conhecimento por parte de hackers de modos de invasão de sistemas informáticos fazem com que a probabilidade de violações de dados e necessidade de responsabilização seja superior. Antes havia é certo menos preparação e conhecimento sobre o que podia levar a ocorrerem, mas havia também menos envolvimento com capacidade para interferir.

Os responsáveis pelo tratamento são quem em primeira e principal linha tem a obrigação de cumprir todas as normas, decisões, pareceres ou recomendações que são dadas pelas autoridades de controlo e de perceber que o que tem de ter sempre em consideração que a responsabilidade é sua e quanto mais cumprirem com tudo o que está ao seu alcance menor será a sua possível responsabilização. Não é demais referir que apenas com uma atuação

proativa e sempre tendo em conta o que está em causa é que podemos ter uma evolução digital de acordo com o que nos dias de hoje é identificado como o futuro desejado, virado para a substituição por máquinas de algumas tarefas feitas por pessoas. A Administração Pública não pode prosseguir e assumir uma postura de administração aberta, com todos os benefícios associados e mencionados anteriormente, se não tiver no seu seio quem tenha a consciência e mentalidade necessária sobre a importância da sua atuação, que cooperem de acordo com essa importância e que tenham em consideração que quanto mais respeitarem todas as normas que lhes sejam impostas, tornar-se-á possível que seja visto com bons olhos o progresso digital tal como a sociedade precisa. A cooperação entre os responsáveis e a autoridade de controlo nacional, a CNPD, é o primeiro passo no caminho certo pelo respeito pelos direitos e interesses dos titulares dos dados e para o cumprimento da legislação europeia e só havendo este aproveitamento de todos os recursos disponíveis é que podemos continuar a falar em inteligência artificial, nos benefícios que atos automatizados podem ter, na celeridade “digital” e todos os outros benefícios que têm sido referidos.

3.2.1. Entidades competentes a nível da União Europeia

Na União Europeia há a recolha de dados dos cidadãos europeus por parte dos órgãos, organismos e instituições que a compõe, havendo uma responsabilização assumida que lhes impõe que sejam o exemplo daquilo que se pretende que seja a atuação no seio de cada Estado-Membro. Basta pensarmos que a mencionada administração aberta implica que haja uma aplicação de normas que permitam que não sejam os próprios órgãos e organismos da União a não permitirem que a mesma seja possível devido à elevada probabilidade de incidentes ocorrerem e de dados de cidadãos de vários Estados-Membros sejam postos em causa e que os benefícios que se espera obter sejam pouco relevantes face às desvantagens que podem acarretar. A quantidade de dados que circula no seio da União é elevadíssima e consequentemente a existência de uma partilha indevida ou de haver uma modificação ou perda que não corresponde, como evidente, ao que o titular dos dados queria e tinha interesse é mais provável de ocorrer.

Esta dimensão de quantidade de dados impõe que exista um conjunto de entidades que não só sejam quem é hierarquicamente superior às entidades de cada Estado-Membro, mas também que atuam no sentido de a própria União Europeia ser uma referência de como o tratamento de dados deve ser feito. São elas que perante os dados que circulam no seu seio tomam as decisões

de como é que se vão moldar de forma a conseguirem sempre cumprir com os seus objetivos no que se refere ao crescimento digital que se vêm assistindo. Quando se aborda este tópico estamos a falar de entidades como a mencionada autoridade de controlo europeia, a Autoridade Europeia para a Proteção de Dados (AEPD), e das autoridades públicas independentes da União Europeia.

A AEPD assume diversas funções que se dividem em três pilares: controlo, aconselhamento e cooperação. Todas as funções que assume tem como objetivo a proteção dos dados, assegurar que as instituições e órgãos comunitários respeitam o direito à vida privada quando procedem ao tratamento de dados pessoais ou quando definem novas políticas que podem de algum modo interferir com o respeito pelo direito fundamental dos cidadãos e saber como agir em caso de violação de dados. Foi elaborado para o efeito o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018⁸⁶, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados que veio prever as normas aplicáveis aos órgãos, organismos e instituições em matéria de tratamento de dados pessoais por parte da União Europeia. Com a interoperabilidade que se foi assumindo tornou-se necessário adequar as normas de proteção de dados pessoais ao próprio seio da União. Coopera, ainda, com as autoridades de controlo nacionais de cada Estado-Membro e atua como sua autoridade máxima do cumprimento do RGPD, controlando que a conformidade com a lei e o modo como devem reagir a violações de dados e aconselham sempre que existe alguma questão sobre o impacto que o tratamento de determinados dados terá sobre os titulares dos dados, que medidas técnicas e organizativas devem ser tomadas e responde a alguma questão interpretativa de normas ou aplicação das mesmas a casos concretos.

A atuação da AEPD, em conjunto com o Comité Europeu para a Proteção de Dados, passa também por ser a entidade a quem os encarregados de proteção de dados europeus recorrem sempre que ocorre uma violação de dados num órgão ou instituição europeia de forma a lhe comunicar da sua ocorrência, dos dados que foram afetados e se houve ou tem que haver comunicação ao titular dos dados, atuando deste modo como verdadeira autoridade de controlo em primeira linha. Os encarregados de proteção de dados atuam em cada órgão e instituição como autoridade no cumprimento das normas de proteção de dados e são quem assume a

⁸⁶ Este Regulamento vem revogar o Regulamento (CE) n.º 45/2001 do Parlamento Europeu e pode ser consultado em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725>.

responsabilidade de garantir que há o cumprimento das normas por parte dos responsáveis pelo tratamento. Estes podem ver neles o seu superior hierárquico que os vai controlar e impor como devem atuar e cumprir com as obrigações impostas pelo regulamento geral sobre a proteção de dados. Funciona como um intermediário que identifica os casos que podem levar a um incumprimento do regulamento ou à ocorrência de uma violação de dados, notifica a AEPD e esta agirá em conformidade⁸⁷.

3.2.2. Entidades competentes a nível nacional

Cada Estado-Membro atua em conformidade com o que é imposto no RGPD quer nas interações que existem entre órgãos e entidades nacionais quer quando há uma entidade que atua em vários Estados ou várias entidades interagem entre si no seio da União. Esta interação apenas é possível caso haja um supervisionamento por parte das autoridades de controlo independentes criadas por cada Estado que garantam que em todos os momentos de atuação e de cumprimento das suas finalidades há uma garantia de que os dados se encontram protegidos. O artigo 4.º do RGPD dá umas luzes iniciais do que pode ser uma autoridade de controlo e remete-nos no seu n.º 20 para o artigo 52.º e prevê que a União Europeia, respeitando a soberania nacional e o princípio de subsidiariedade, reconhece a cada Estado a competência de determinar quem atuará como autoridade de controlo no seu país em matéria de proteção de dados. Este entendimento deriva do conhecimento de que em termos de proteção de dados é melhor que seja uma autoridade nacional a proteger os direitos e interesses do titular dos dados e não uma autoridade única para todos os Estados-Membros. É uma matéria sensível e que requer que todas as decisões tomadas quer para o seu progresso quer para a sua defesa devam ser sempre tomadas da melhor forma possível e de forma a que os riscos sejam os menores possível para o titular dos dados⁸⁸. O n.º 1 do artigo 51.º determina que será uma ou mais autoridades públicas independentes que irão assumir a responsabilidade de, em cooperação com as autoridades escolhidas pelos outros Estados-Membros e com a Comissão, n.º 2 do referido artigo, assumir todas as ações necessárias para que o regulamento, o RGPD, seja cumprido. Esta cooperação no cumprimento das normas torna-se essencial para que a interação mencionada entre diferentes entidades seja possível e para que haja um entendimento de como

⁸⁷ Orientações gerais que podem ser retiradas do https://www.edps.europa.eu/sites/default/files/publication/brochure_2009_pt.pdf.

⁸⁸ COUTINHO, Francisco Pereira, "A independência da Comissão Nacional de Proteção de Dados", in Francisco Pereira Coutinho *et al.* (ed.), *Anuário da Proteção de Dados*, Lisboa, CEDIS, 2020. O artigo 1.º do Tratado da União Europeia consagra o princípio da subsidiariedade e determina que as decisões sejam sempre tomadas o mais próximo dos cidadãos.

deve funcionar esta circulação de dados entre entidades com níveis diferentes de tecnologia e com uma capacidade diferente de procederem ao tratamento dos dados que recolhem.

As autoridades públicas independentes assumem um papel de superior hierárquico de todas as autoridades, entidades ou outras figuras que assumam o papel de responsáveis pelo tratamento. São autoridade máxima em cada Estado-Membro e representam a atuação do mesmo em comparação com os outros Estados e na necessidade de coordenação no tratamento de dados que circulam com a existência de uma administração aberta. Atuam sempre de modo independente⁸⁹, não podendo outras autoridades, entidades ou mesmo o Estado interferir na atuação e decisões tomadas pelas autoridades⁹⁰. O mesmo se exige aos próprios membros da autoridade, ao se impor que, apesar de puderem desempenhar outras funções que não se relacionem com o cargo, não o poderão fazer caso isso represente uma incompatibilidade dada a responsabilidade das funções que assumem e da dimensão que representam. Se desempenharem outras funções que influenciem a sua opinião sobre um determinado assunto que está a ser discutido no momento isso retiraria ao membro em questão uma opinião sua e adequada ao que se está a determinar, devendo o mesmo ser considerado como potenciador de conflito de interesses. Todos os Estados têm de garantir que estas autoridades são de facto independentes em todos os aspetos da sua atuação e composição e que nada, mesmo havendo um controlo financeiro que as financia, afeta direta ou indiretamente o rumo que a autoridade determinar como sendo o melhor para si e para o cumprimento das suas funções. Os seus membros⁹¹ são determinados de acordo com esta ideia e não outras regras que poderiam de algum modo interferir nas decisões que seriam tomadas⁹². Se houver uma influência de quem são os membros desta autoridade, há a possibilidade de todas as decisões que são tomadas por ela tem de alguma forma uma alteração e interferência num sentido que não seria adotado se não estivessem esses membros. Não quer com isto dizer que a decisão tomada seria incorreta, mas sim que poderia ser potenciadora de riscos ao não controlar determinada entidade como manda o regulamento ou não impor medidas de controlo mais rígidas a determinada entidade

⁸⁹ O Acórdão Comissão Europeia vs Áustria C-614/10, 16 de outubro de 2012 foi um dos acórdãos que abordou a questão da necessidade de existir uma independência total das autoridades de controlo no domínio de exercício por parte dos membros da autoridade de outras funções. O conceito de total independência foi posto em questão quanto ao seu âmbito de abrangência. O que se entendia de total independência não era totalmente claro e tornou-se evidente que o desempenho de mais do que uma função dependia de uma investigação sobre o modo como a parcialidade desse membro iria ser afetada e que outra função e onde iria ser desempenhada. Não era claro que à partida o desempenho de mais do que um emprego fosse prejudicial para a imparcialidade do membro, contudo gerou-se a dúvida. Concluiu-se que através de uma perceção sobre a influência direta ou indireta que possa existir com a acumulação de cargos é perceptível que parcialidade possa existir. No caso concluiu-se pela negativa quanto à parcialidade.

⁹⁰ Artigo 52.º do RGPD.

⁹¹ Artigo 53.º do RGPD consagra quem pode nomear os membros.

⁹² N.º 4, 5 e 6 do artigo 52.º do RGPD.

devido a uma ligação subjetiva entre os membros da autoridade de controlo e a entidade que está a ser controlada⁹³.

Os Estados-Membros têm a legitimidade de reconhecer à sua autoridade de controlo outras funções que não as previstas nos três primeiros números do artigo 58.º de forma a, tal como refere o n.º 5 do artigo mencionado, abrir portas para a autonomia e soberania de cada Estado em moldar a atuação da autoridade de controlo de acordo com aquilo que se revela adequado para a sua realidade e que melhor se enquadra com a atuação que se espera por parte da guardião do RGPD. Nem todos os Estados estão ao mesmo nível de desenvolvimento em termos tecnológicos e de digitalização dos seus serviços e nessa medida exigem do seu legislador níveis diferentes de previsão legal, assim como, uma compreensão consciente de que a autoridade de controlo tem de ter os meios legislativos que acompanhem a exigência de controlo que os seus responsáveis pelo tratamento exigem. Se temos um país que tem mais capacidades económicas de ter meios digitais, ou mais meios digitais, será necessário reconhecer às autoridades de controlo normas que permitam que essa evolução tecnológica seja feita de acordo com a lei da União e que essa evolução seja possível através da perceção, na linha do que já foi mencionado antes, de que só pode ocorrer caso seja demonstrado que apesar dos riscos que representa, as vantagens e a proteção legislativa existem e estão empenhadas em tomar todas as precauções necessárias para mitigar os riscos existentes. Se a evolução tecnológica dos serviços ou de obtenção de um bem, por outro lado, estiver apenas numa fase ainda pioneira em que a aposta ainda se revela com pouca adesão e é vista como uma realidade ainda distante face a outros Estados, não se justifica que este Estado vá para além do que é o mínimo e do que o regulamento impõe.

Uma autoridade sem os meios legislativos necessários por falta de abertura da União para que o seu Estado possa suprir as suas necessidades legislativas seria e teria a sua atuação demasiado limitada e comprometeria a sua capacidade de ser aquilo que se comprometeu a ser. Como é que um Estado pode evoluir e cumprir ao mesmo tempo a legislação europeia se não consegue demonstrar ao titular dos dados que tem todas as capacidades para adotar todas as medidas técnicas e organizativas que precisa e todos os poderes necessários para o fazer por se encontrar limitado por padrões ideais previstos para se adequar a um universo vasto de realidades. Os titulares dos dados são a chave impulsionadora para que haja a motivação para

⁹³ MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais*, op.cit., página 155.

um Estado apostar na digitalização e para que possa haver a previsão de meios que correspondam ao nível de exigência digital. Há a vontade de evoluir, como foi mencionado antes, mas essa evolução é feita a partir da necessidade de os cidadãos em alcançar novas metas de desenvolvimento e com a confiança e recurso a essas mesmas metas. Um Estado-Membro que tem a perceção de que a digitalização ainda se encontra num estado inicial e de que é necessário apostar financeiramente em meios tecnológicos, não consegue atingir exigências de cumprimento de metas em termos de proteção de dados. Nesse sentido se não houver a transmissão de segurança, através de meios e poderes reconhecidos legislativamente a quem tem a competência de a transmitir, não há as bases necessárias para que possa ocorrer.

As autoridades de controlo atuam no cumprimento de todas as normas e princípios que devem ser cumpridos por todos os responsáveis pelo tratamento e nesse sentido um dos pontos a ser cumprido é o cumprimento do princípio da segurança e o princípio da lealdade. A nossa autoridade só consegue cumprir o princípio da segurança e o princípio da lealdade se conseguir ter a capacidade legislativa⁹⁴ de conseguir advertir, corrigir ou investigar a atuação dos responsáveis pelo tratamento e perceber se tem as medidas previstas para o exercício de direitos do titular dos dados. Como é que conseguiria a autoridade de controlo perceber se atuação de um determinado responsável está de acordo com os princípios mencionados se não tivesse os poderes necessários para adotar todas as medidas de investigação necessárias e se uma vez averiguado que não cumpre os princípios mencionados não pudesse tomar as medidas de acordo com os resultados dessa mesma investigação. Como é do conhecimento de todos a palavra preferida dos juristas, ou uma das, é “depende”, cada caso é um caso e nesse sentido cada exigência da vida prática é diferente. Se a autoridade de controlo estivesse limitada nos poderes que lhe são reconhecidos poderia não ter a legitimidade para atuar da melhor forma para garantir a transparência adequada e a confidencialidade adequada para cada titular de dados e caso concreto. Uma atuação de qualquer autoridade que desempenhe funções numa matéria que pode ser de conteúdo muito variável é uma autoridade com uma limitação evidente e aquém das suas capacidades e necessidades para ter um desempenho de acordo com as suas expectativas e determinação de proteger o titular dos dados e agir da melhor maneira possível.

⁹⁴ E neste sentido para além dos poderes que são reconhecidos pelo RGPD às autoridades de controlo existe um conjunto de outros poderes que lhe são reconhecidos pela Lei n.º 58/2019 e que alargam o leque de competência que é reconhecido pelo RGPD. Há deste modo a nível nacional o entendimento que pode a CNPD atuar em mais âmbitos do que aqueles que lhe são reconhecidos pela lei que deu base à nacional.

A atuação desta autoridade de controlo tem ainda de ser pautada pelo princípio da proporcionalidade e sempre tendo em conta que antes que seja concluída qualquer ideia sobre um determinado ato que ocorreu deve ser ouvida a parte que agiu em desconformidade, ou suposta desconformidade, de modo a que seja percebido o que ocorreu e para que haja oportunidade de defesa. Depois de ouvida a parte e com as provas reunidas é que se pode concluir sobre o que se passou e que medidas é que devem ser tomadas de modo proporcional. Não podem ser assumidas como verificadas as provas que são observadas pela autoridade ou que parecem demonstrar que determinados atos poderão vir a se verificar. O considerado 129 do RGPD prevê que “Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com o presente regulamento, tendo em conta as circunstâncias de cada caso concreto, respeitar o direito de todas as pessoas a serem ouvidas antes de ser tomada qualquer medida individual que as prejudique, e evitar custos supérfluos e inconvenientes excessivos para as pessoas em causa”.

Tendo cada Estado-Membro a(s) sua(s) autoridade(s) de controlo e tendo todas o mesmo objetivo, cumprimento do RGPD no seu Estado, torna-se essencial que todas ajam de certo modo em conjunto e consigam mutuamente se ajudar no cumprimento desse mesmo objetivo. Se há uma União, legislação, órgãos e instituições comuns então também deve haver uma cooperação no sentido de otimizar a atuação e permitir que, para além do cumprimento do objetivo mencionado, haja uma atuação igual ou muito parecida e permita que assim como há a circulação de bens e pessoas, haja também uma circulação de entendimentos sobre casos concretos que possam de certo modo ter mais do que uma resposta. Os cidadãos ao denotar esta unificação de atuação confiam mais na recolha dos seus dados pessoais, consequentemente permitindo que a administração aberta possa existir e que possa ser o caminho a seguir como já foi mencionado inúmeras vezes anteriormente. Quando o cidadão europeu permite uma recolha dos seus dados pessoais num Estado diferente do seu Estado-Origem tem que ter a confiança de que os seus dados serão tratados exatamente do mesmo modo que seriam quando os partilha no seu Estado de origem.

O nosso Estado-Membro decidiu ter apenas uma autoridade de controlo independente sendo ela a Comissão Nacional de Proteção de Dados (CNPd) que atua em todo o território e controla todos os responsáveis pelo tratamento de todas as entidades portuguesas. Esta autoridade desempenha as funções enumeradas anteriormente em nome do nosso Estado, atuando sozinha no cumprimento dessas funções.

3.2.2.1. Comissão Nacional de Proteção de Dados

A Comissão Nacional de Proteção de Dados (CNPd) é uma entidade administrativa independente⁹⁵ que desempenha funções junto da Assembleia da República em matéria de proteção de dados e cumprimento do Regulamento (UE) n.º 679/2016, de 27 de abril, tendo de assegurar que todas as entidades públicas e privadas a quem pede a colaboração cumprem as disposições de regulamento em todos os atos que pratiquem que tenham no seu conteúdo dados pessoais⁹⁶. Devem as entidades, independentemente do seu estatuto ou posição hierárquica colaborar com a CNPD atuando em conformidade com o regulamento e demonstrando que o fazem sempre que lhes é requerido. Os direitos, liberdades e garantias dos titulares de dados são a prioridade de atuação da CNPD e a independência de atuação que lhes é reconhecida deve ser sempre com o objetivo de os ter em consideração e os proteger o melhor possível em cada situação⁹⁷. A CNPD atua deste modo como auxiliar no cumprimento das normas e como controladora do seu cumprimento em qualquer tratamento de dados que ocorra.

Esta Comissão foi constituída com um propósito inicial, que depois se tornou a sua principal finalidade, de implementar todas as medidas e atos que se revelam necessárias, adequadas e proporcionais para a transposição do Regulamento sobre a Proteção de Dados no nosso ordenamento jurídico e de cooperar com a União Europeia para a digitalização das suas sociedades e economias. Este processo foi demorado em Portugal, tornando-nos um dos últimos Estados a implementar o regulamento, tendo esta demora existido pelo facto de haver uma recusa por parte da CNPD em aplicar determinadas normas previstas na Lei de Execução do Regulamento aplicável a todos os Estados-Membros. Esta recusa não foi vista com bons olhos e levou a que se considerasse que algumas dessas recusas eram injustificáveis e não podiam ocorrer mesmo sendo feitas por uma autoridade administrativa independente. A independência

⁹⁵ As autoridades nacionais em matéria de controlo de aplicação do RGPD têm de ser sempre caracterizadas pela sua independência. É de tal modo importante que o sejam que o RGPD consagra que tem que agir “com total independência”, n.º 1 do artigo 52.º do RGPD.

⁹⁶ Este título é-lhe reconhecido apenas a ela, CNPD, não tendo Portugal escolhido a possibilidade de ter mais do que uma entidade competente nesta matéria. O artigo 3.º da Lei n.º 59/2019, lei de execução do RGPD, reconhece-a como tal, não fazendo menção a outra autoridade. Nos artigos seguintes consagra as suas características e modo de atuação.

⁹⁷ Artigo 4.º, 2) da Lei n.º 58/2019, de 8 de agosto.

reconhecida legalmente a esta Comissão não lhe permitia, segundo determinados entenderes, que pudesse simplesmente atuar como desejava e não aplicasse determinadas normas sem que para isso tivesse uma motivação. Por outro lado, considerou, na sua análise à lei de execução⁹⁸, que muitas das disposições eram desrespeitosas do Direito da União Europeia e que nesse sentido não faria sentido estar a cumprir uma lei ilegalmente constituída. A questão que se colocou na altura, e que ainda hoje passados 5 anos ainda se coloca, é de saber se pode uma autoridade recusar-se a aplicar determinadas normas com o fundamento de não concordar com as mesmas e sob a legitimidade de ser uma autoridade independente, até onde vai a independência de uma autoridade independente, quais os limites e se algum órgão a controla.

Esta autoridade é essencial e o seu papel como guardião do RGPD é constantemente posto à prova, quer através de pareceres, decisões, deliberações ou em tribunal, sempre que é necessário haver uma reflexão e opinião dominante e esclarecida sobre um determinado ponto, matéria, em que a lei não é tão clara como deveria ser para aquele caso concreto, visto que o legislador por muito que pense em todos os casos concretos que possam surgir no dia-a-dia não consegue prever, nesta matéria, e em todas as outras que compõe qualquer ordenamento jurídico, todos os pormenores que caracterizam ou podem caracterizar um caso concreto. Dois casos podem ser semelhantes, mas terem um detalhe que os diferencia e ser esse detalhe num dos casos que leva a que seja preciso uma pronúncia por parte da CNPD. Ou, por outro lado, podemos ter circunstâncias sociais que nunca surgiram nem são possíveis de prever, como a pandemia do Covid-19, que revelam que apesar de haver uma previsão de meios digitais não havia ainda perceção de como é que a recolha de dados poderia ocorrer com a utilização de aplicações como a aplicação do Covid-19 e a necessidade de os serviços públicos continuarem em funcionamento através de sistemas informáticos. O Covid-19 foi um momento em que se valorizou a atuação da CNPD e se exigiu que houvesse capacidade de resposta para todas as questões que iam surgindo à medida que a sociedade funcionava apenas ou praticamente apenas com mecanismos à distância e que obrigava, como vimos no ponto 1, a uma adaptação dos serviços. Em termos de jurisprudência podem determinadas decisões da CNPD ou pareceres da mesma ser questionados quanto à sua aplicabilidade a um caso concreto ou podem ser chamados a pronunciar-se quanto a um determinado ponto de forma a que possam ser uma espécie de fonte legislativa que tenha influência na perceção dos detalhes do caso concreto e na

⁹⁸ A lei de execução é a Lei n.º 58/2019 de 8 de agosto, como lei que transpõe o Regulamento no nosso ordenamento jurídico e que visa o seu cumprimento. As normas que a compõe refletem e remetem para o Regulamento, sendo o espelho do que nele se prevê.

aplicabilidade de normas à resposta jurídica necessária. É chamada deste modo para ser “a voz decisora” em momentos de indecisão ou como esclarecedora de pontos que podem influenciar a decisão que está a ser tomada. Este papel que assume foi o principal motivo para se considerar muito grave a posição adotada pela CNPD quanto à lei de execução, como foi mencionado antes, visto que, como é que a autoridade responsável máxima se recusa a exercer o papel que lhe foi reconhecido constitucionalmente e no Tratado para o Funcionamento da União Europeia? Ao não querer aplicar certas normas da lei de execução está de forma clara e inequívoca a não transpor o direito da união na totalidade e com isso a descredibilizar a sua autoridade. Como é que se iria cumprir o que a autoridade administrativa independente impunha se ela própria não cumpria com o que o RGPD determinava? Gerou muita controvérsia e fez com que se duvidasse da sua capacidade e legitimidade de atuação⁹⁹.

Embora haja o entendimento de que o melhor é uma atuação nacional e de que esta atuação é independente, a verdade é que cumpre à CNPD uma atuação sempre em cooperação com a União, com os seus órgãos e com a legislação que a legitima como autoridade. Há aqui a presença de uma cooperação leal entre as autoridades de cada Estado-Membro e a União Europeia que se revela imprescindível para que possa cada Estado evoluir. Cada uma das autoridades age no interesse dos seus cidadãos, mas sempre em conexão, não dependente, com o que são as linhas de atuação, entendimento e vontade da União Europeia¹⁰⁰. A sua atuação como autoridade de controlo é diferente de outras autoridades administrativas independentes, visto que atua quase como se fosse uma agência europeia apesar de serem autoridades nacionais, e consequentemente aumenta também a sua responsabilidade e consciência da sua importância. Esta autoridade, como já foi mencionado antes, precisa da cooperação das entidades, do Estado-Membro, para que possa exercer as suas funções e sabemos que sem a existência da União e dos seus mecanismos não é possível a um Estado alcançar determinadas metas de desenvolvimento e evolução por falta de meios económicos para tal¹⁰¹. O RGPD tem aplicabilidade direta, tem uma lei que a transpõe para o nosso ordenamento, mas isso não retira

⁹⁹ Bacelar de Vasconcelos considera que o “direito à resistência” apesar de existir não pode ser um fundamento de desrespeito e desconsideração pelo Direito da União Europeia.

¹⁰⁰ Podem ser consultadas em https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm as várias autoridades de controlo que existem na União Europeia, encontrando-se este site dividido por Estado-Membro com as informações básicas de cada autoridade nacional de controlo.

¹⁰¹ Portugal com a adesão à União Europeia, tal como os outros Estados, teve a possibilidade de crescer economicamente e de conquistar patamares de desenvolvimento que não conseguiria ou em outros casos teria bastantes dificuldades em conseguir e demoraria muito tempo a fazê-lo. Esta autoridade tem por isso a responsabilidade de garantir que há um aproveitamento dos meios dados pela União ao cumprir com os pressupostos de proteção dos dados pessoais. Os Estados se não trabalharem em conjunto para a proteção dos dados não conseguirão que os progressos que se quer alcançar sejam conseguidos. A administração aberta, benéfica para os cidadãos e para os Estados, só consegue funcionar se houver um cumprimento legal.

a importância e percepção de que sem um empenho de todos elementos num Estado, nada disso adianta.

3.2.2.1.1. Funções das autoridades de controlo

O RGPD prevê uma lista extensa das funções/competências/atribuições que são reconhecidas à CNPD e que reunidas constituem aquilo que se espera que uma autoridade responsável pelo tratamento de dados execute, em síntese a função de guardião do RGPD. A atuação de uma autoridade com esta dimensão e importância tem de ter de forma precisa a delimitada as funções que assume, tendo de haver uma proporcionalidade da responsabilidade que assume. O artigo 58.º RGPD e a lei nacional de cada Estado em matéria de proteção de dados preveem quais são essas funções e dentro de cada uma quais as atividades que pode desempenhar¹⁰² sendo estas funções apenas exemplificativas e não absolutas daquilo que em concreto é esperado da CNPD. As leis nacionais têm um papel muito importante não só como cumpridoras da lei europeia, mas também como criadoras de normas ou recomendações que complementem esta lei e que façam com que a atuação das autoridades seja em conformidade com a lei, mas também com as características e necessidades de cada Estado, como vimos anteriormente. Nem todos os países que compõe a União Europeia são iguais em termos de desenvolvimento digital e nesse sentido as autoridades de controlo terão de ter em conta essas diferenças e reajustar-se às mesmas. O legislador nacional tem conhecimento de que deve fazer uso da soberania nacional que lhe é reconhecida e reunir num diploma todas as normas que consigam o melhor dos dois mundos, ou seja, que consiga cumprir e ter vantagens com o que a digitalização traz em termos daquilo que a lei europeia prevê e ao mesmo tempo saber como pode criar normas que complementem e ajudem neste acolhimento das vantagens.

3.2.2.1.2. Poderes de investigação

O n.º 1 do artigo 58.º do RGPD consagra que são reconhecidos à CNPD poderes de investigação quanto aos atos praticados por quem tem a obrigação de fazer cumprir o RGPD. Os responsáveis pelo tratamento de dados e os subcontratantes, que em nome deste atuam, nos casos em que existam, tem o dever de cumprir com todas as obrigações que o RGPD lhes impõe, cabendo à autoridade de controlo, a CNPD, encarregar-se de garantir, como superior hierárquica,

¹⁰² Todos os Estados-Membros tem os mesmos poderes, com o mesmo alcance e objetivos, de acordo com o RGPD, não podendo haver diferenciação entre os Estados quanto à atuação das autoridades de controlo por eles nomeadas. Todas desempenham a função de proteção do RGPD e de garantia de cumprimento de todas as normas do RGPD. Para que os cidadãos europeus tenham os seus dados protegidos em qualquer circunstância tem de essa proteção ser igual em todos os Estados. Para que possamos falar em administração aberta na União tem de haver a garantia de que os dados que um Estado partilha com outro não põe em nenhum momento em causa os mesmos já que esse Estado terá uma autoridade de controlo com a mesma capacidade de atuação e proteção desses dados.

que esse cumprimento ocorre e de acordo total com todas as especificidades que as compõe. A CNPD tem o direito de controlar os responsáveis pelo tratamento ou outras entidades, mas ao mesmo tempo tem o dever de o fazer, tem de garantir que tem conhecimento de todas as atividades de tratamento que se encontram na sua jurisdição. Não basta apenas esperar que cumpram o RGPD ou de agir em caso de risco, mas sim ter também, tal como o responsável pelo tratamento, um comportamento proativo, preventivo e informado sobre todos os dados que são recolhidos pelas entidades a si subordinadas. É quem tem a responsabilidade máxima de, perante a União Europeia e o titular dos dados pessoais, demonstrar que apesar dos esforços pela eliminação dos riscos, estes não foram possíveis de eliminar naquele caso em concreto e o indesejado acabou mesmo por ocorrer.

Toda a atividade tem de ser pautada por uma comunicação permanente entre a CNPD e o responsável pelo tratamento que está a ser supervisionado e investigado de modo a que saiba o que se está a tentar perceber e de que modo pode contribuir para a demonstração da sua realidade quanto aos dados que recolheu e de forma a identificar os possíveis problemas que terá de corrigir e sob os quais poderão ser aplicadas coimas. Por outro lado, pode o responsável não concordar com o que está a ser concluído e ter a necessidade de se defender apresentando os fundamentos necessários para isso e ajudando também deste modo a uma atuação mais célebre da autoridade de controlo.

3.2.2.1.3. Poderes de correção

A CNPD desempenha de igual modo funções de correção, que derivam de observações que foram feitas no decorrer do exercício dos seus poderes de investigação, sendo estes de modo explicativamente previstos no n.º 2 do artigo 58.º, sempre que considerar como necessários, adequados e proporcionais ao caso concreto e com o intuito de melhorar a atuação do responsável pelo tratamento e prevenir que efeitos negativos se possam mesmo verificar. Os poderes de correção podem compreender atos de advertência ou ordens no sentido de alteração de determinados comportamentos, não havendo deste modo apenas correção de um comportamento que já existiu ou que está na iminência de ocorrer. Podem ser tomadas medidas mais graves nos casos em que se decide que a certificação que foi reconhecida e atribuída a uma determinada entidade¹⁰³ deve ser retirada por terem praticado algum ato desconforme com

¹⁰³ Encontram-se previstos os seus termos nos artigos 42.º e 43.º do RGPD.

o imposto como requisitos para que uma certificação seja atribuída¹⁰⁴. Pode ainda aplicar uma coima por algum dos atos praticados de acordo com as alíneas anteriores à alínea i) do n.º 2.

Um dos poderes de correção mais importantes que a autoridade de controlo tem a desempenhar é a de ordenar ao responsável pelo tratamento que comunique aos titulares dos dados que houve um incidente com os seus dados e quais as consequências e precauções que existem e que devem ser postas em prática caso o responsável pelo tratamento ainda não o tenha feito. Por outro lado, como já foi mencionado anteriormente são quem recebe as reclamações dos titulares dos dados, o que lhes impõe que atuem em conformidade e percebam o fundamento das reclamações e a sua veracidade.

3.2.2.1.4. Poderes consultivos e de autorização

A CNPD desempenha ainda poderes de consulta e autorização de atos que estejam a ser estudados pelos responsáveis pelo tratamento, como melhorias do seu tratamento ou dúvidas sobre como devem proceder num determinado caso de modo a que o seu tratamento seja o mais protetivo dos dados pessoais possível, como possíveis atos a praticar. O desempenho destas funções é feito através de consultas prévias a pedido dos responsáveis, através de pareceres requeridos ou que a CNPD entendeu como necessários e relevantes. Os responsáveis pelo tratamento nem sempre tem o conhecimento de como determinado ato que pretende praticar poderá de alguma forma pôr em causa os dados pessoais pelos quais é responsável e por vezes precisa que haja também um reconhecimento superior de que pode praticar determinados atos.

3.2.2.2. Encarregado de proteção de dados

A nomeação de um Encarregado da Proteção de Dados existe como obrigação em determinados casos, tais como, entre outros, os casos em que estamos perante uma autoridade ou um organismo público. A Administração Pública tem de nomear sempre um Encarregado da Proteção de Dados independentemente dos dados pessoais que trata e dos riscos que estão presentes. A obrigatoriedade de haver a nomeação de um Encarregado da Proteção de Dados advém da Diretiva de 95 em que se previa como um dos requisitos para a sua existência era haver um encarregado de proteção de dados, tendo em consideração o número de trabalhadores que as componha. Atualmente este critério não é aplicado dado que se considerou, e bem, que não é o número de trabalhadores que uma entidade tem que deve e determina o risco do

¹⁰⁴ Sabemos que as câmaras de videovigilância tinham que ter uma autorização da CNPD para que pudessem existir e ser autorizadas a recolher imagens. A autorização era feita relativamente ao número existente de câmaras e à direção da sua imagem. Caso houvesse uma alteração com o acréscimo de mais câmaras ou com a mudança de direção da mesma, a autorização deixava de existir.

tratamento de dados, dado que, uma entidade com poucos trabalhadores, mas com determinadas funções e tratamento de dados pode representar mais risco. Tudo depende do tratamento que cada entidade faz, e não o número de trabalhadores, das medidas técnicas e organizativas e de que modo avalia o impacto de uma nova atividade de tratamento que pretende pôr em prática.

Estando perante uma autoridade ou organismo da Administração Pública entende a lei, alínea a) do n.º 1 do artigo 37.º do RGPD, que o simples facto de terem um elemento que se enquadra no RGPD, o tratamento de dados pessoais para a prestação de um serviço, é motivação suficiente para a obrigação da nomeação do Encarregado da Proteção de Dados independentemente se trata apenas dados pessoais básicos ou de poucos dados pessoais. Não há qualquer verificação de preenchimento de critérios, tal como ocorre com os restantes tratamentos de dados, para que a obrigação seja criada. Contudo, há que assinalar que a parte final da alínea a) do n.º 1 do artigo 37.º do RGPD faz a ressalva que não há esta obrigação quando falamos de tribunais ou autoridades judiciais, visto que, estes, apesar de teoricamente terem esta obrigação, a verdade é que não faz sentido o terem devido ao princípio da independência que lhes é reconhecido. Não podem ser influenciados ou obrigados a atuar de um determinado modo e comprometer a sua atuação de acordo com o que se revela como verdade e juridicamente justo devido ao que um determinado encarregado lhes diz como devem fazer.

Para os demais responsáveis pelo tratamento, que não pertencem à Administração Pública, é necessário que esteja preenchido um de dois critérios para que esta obrigação exista. As alíneas b) e c) do n.º 1 do artigo 37.º determinam que caso a natureza, âmbito ou finalidade justifiquem que haja um maior controlo por parte do titular dos dados ou quando for um tratamento em grande escala de dados pessoais sensíveis tem de haver obrigatoriamente a nomeação de um Encarregado da Proteção de Dados.

A diferença entre as exigências legais de acordo com quem assume o papel de responsável pelo tratamento parece justificado pelas responsabilidades que são assumidas por cada um dos responsáveis pelo tratamento, não sendo possível equiparar o gerente de uma empresa com uma autoridade ou entidade pública. Podem os dois recolher os mesmos dados pessoais e recorrer aos mesmos meios informáticos para o fazer, contudo, a quantidade de dados será certamente superior e consequentemente a responsabilidade assumida será na proporção dessa

quantidade de dados. A imposição legal da União quanto às entidades e circunstâncias do tratamento de dados que cada uma desempenha não impede, segundo o n.º 4, que haja por parte de cada Estado a consagração de outras circunstâncias em que se imponha a obrigatoriedade de haver um encarregado da proteção de dados. Não há por parte da União uma imposição dos casos em que tem de haver uma nomeação deixando deste modo a possibilidade de cada Estado adaptar este aspeto às suas particularidades, havendo o respeito pela soberania que tem e de forma a que possam corresponder às particularidades da sua realidade social. A limitação às três primeiras alíneas do artigo 37.º seria assumir que mesmo que um Estado estivesse perante um caso que na prática se revelasse suscetível de riscos não pudesse impor esta obrigatoriedade e deste modo poderia estar a ser imprudente para com os seus cidadãos, não podendo estes agir de alguma forma contra o seu Estado.

3.2.2.3. Responsável pelo tratamento

Ao longo do texto foi mencionado e referido em vários momentos e devido a vários fundamentos o responsável pelo tratamento dos dados como o principal e único responsável pelo tratamento e proteção dos dados pessoais, mesmo nos casos em que contrate um subcontratante para atuar em determinados aspetos em seu nome. Ao determinar que o subcontratante irá cumprir atos em seu nome não exclui a sua responsabilidade pelo que ocorrer aos dados do titular dos dados, visto que, a autonomia do subcontratante não existe na sua atuação com os dados pessoais recolhidos. Foi sendo afluído este papel central e determinante do responsável pelo tratamento ao longo das páginas anteriores, não nos podendo esquecer que é esta a responsabilidade que falamos quando afirmarmos que a digitalização e o conceito de dados pessoais têm que estar sempre protegidos por quem assume a responsabilidade.

Quem é o responsável pelo tratamento dos dados e de que modo assume este a responsabilidade total pelo tratamento dos dados pessoais que lhe são confiados? Consagra o artigo 4.º, 7) do RGPD o que se entende por responsável pelo tratamento e como é feita a sua determinação em todos os casos em que há dados pessoais que precisam de ser protegidos. A determinação de quem pode ser qualificado como responsável pelo tratamento de dados é feita com base em "critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro". A questão que se coloca é que critérios são referência para que determinada entidade possa ser considerada prevista no artigo e número mencionado e cumpra deste modo o direito da união em termos de determinação de competências em matéria

de tratamento de dados pessoais. Os critérios têm de ser restritos e concretos ao estarem a assumir a responsabilidade de determinar quem tem a legitimidade e competência para assumir a responsabilidade de tratamento e proteção, principalmente proteção, de dados tão relevantes, como já foi mencionado anteriormente, como os dados pessoais. Não pode o responsável ser qualquer pessoa ou entidade que entenda que tem a capacidade de adotar todas as medidas que considera necessárias para impedir que haja uma partilha indevida dos dados ou que os mesmos sejam modificados sem o consentimento do titular dos dados ou que haja o desaparecimento dos mesmos sem que seja identificável onde os dados se encontram e o que pode ocorrer com eles, não sabendo deste modo quem tem os dados e/ou a quem os estará a partilhar.

Este é o ponto central em matéria de proteção de dados. Sem a determinação de quem é o responsável pelo tratamento não faz sentido a aplicação das normas em matéria de proteção de dados nem a partilha dos dados. O titular dos dados só deve partilhar os seus dados se souber quem é o responsável pelos mesmos e que medidas técnicas e organizativas adota para a proteção dos dados pessoais que partilha. Este conhecimento não impede, contudo, que haja efetivamente uma partilha indevida ou modificação ou desaparecimento dos dados, já foi mencionado anteriormente que apesar do cumprimento legal e da tomada de medidas ideais e adequadas isso não significa que seja possível eliminar por completo os riscos que a partilha de dados representa. Há sempre riscos mesmo que se adote todos os cuidados que esta matéria exige e mesmo que haja uma determinação clara de quem é o responsável pelo tratamento e de que modo deve este proceder para que a proteção dos dados esteja sempre assegurada. Seria utópico pensar que seria possível essa realidade e de garantir com todas as certezas que independentemente do que ocorresse os dados seriam apenas tratados por quem tem competência para o fazer.

Sendo esta tese centrada no responsável pelo tratamento e assumindo este, por outro lado, um papel determinante em matéria de dados pessoais, torna-se importante perceber muito bem o que se entende quando falamos de responsável pelo tratamento. Só desconstruindo todos os aspetos do seu conceito é que conseguimos posteriormente perceber a responsabilidade que assume e quem o pode controlar no cumprimento dessa responsabilidade.

3.2.2.3.1. Conceito e critérios determinantes do que se entende por responsável pelo tratamento

Na introdução deste ponto já foi sendo dando nuances do que podemos entender como responsável pelo tratamento e como é feita a sua determinação em todos os casos em que ocorre a recolha de dados pessoais. Consagra o artigo 4.º, 7) do RGPD que se entende por responsável pelo tratamento quem se caracterize como sendo uma “a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais”, sendo que, esta determinação ocorre “sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro”. É claro que, através deste conceito, é a lei europeia que consagra o que deve ser considerado como responsável pelo tratamento de acordo com critérios legais e não apenas de acordo com o que cada entidade entende que pode ser. Não há uma escolha linear de quem é o responsável pelo tratamento onde se reconheça que uma entidade se possa considerar como responsável pelo tratamento sem que cumpra nenhum dos requisitos. É uma responsabilidade que só pode ser assumida por quem efetivamente tem os meios para o fazer, possa assumir essa responsabilidade com a serenidade que a matéria o exige e possa efetivamente cumprir com o conceito. São direitos fundamentais que estão aqui em causa e que por isso não pode haver subjetividade na definição de responsabilidade.

O conceito de responsável pelo tratamento pode ser dividido e entendido em três elementos caracterizadores sendo eles (1) o responsável tem de ser uma pessoa singular ou coletiva, sendo esta uma autoridade pública, uma agência ou outro organismo, (2) que pode ser responsável de forma individual ou em conjunto com outro responsável e que (3) define quais são as finalidades do seu tratamento de dados e os meios para as concretizar. Este desdobramento do conceito em três partes faz transparecer que estamos perante um conceito simples e com poucos requisitos e imposições legais, numa primeira e muito superficial análise, para que possa uma entidade ser responsável pelo tratamento de dados pessoais. É importante fazer a menção ao responsável como entidade, como pessoa coletiva, quando o responsável não é uma pessoa singular, visto que neste caso é ela a responsável e não um determinado colaborador dessa pessoa coletiva e desmitifica a ideia de que o responsável tem que ser alguém individualizável. Ninguém assumirá a responsabilidade pelo tratamento indevido a não ser o responsável como pessoa coletiva salvo se utilizar os dados pessoais para finalidades que não as que a entidade

assumiu e neste caso torna-se responsável por esses dados¹⁰⁵. A pessoa singular pode assumir, por legitimidade reconhecida pelo conceito e por serem uma cara que se reconhece esta responsabilidade, mas na verdade na prática são pessoas coletivas que acabam por assumir esse papel.

3.2.2.3.2. O responsável tem de ser uma pessoa singular ou coletiva, sendo esta uma autoridade pública, uma agência ou outro organismo

Quanto a esta primeira especificação podemos desde logo reduzir a complexidade que se poderia esperar nesta matéria, por serem dados que partilhados de forma indevida, alterados ou perdidos trazem consternações ao seu titular de grande relevo, por serem dados que os identificam e individualizam, visto que, parece que não é imposto pela lei nenhum requisito específico para que alguém possa assumir a qualidade de responsável pelo tratamento. Não há uma limitação das entidades que podem assumir essa responsabilidade, não sendo necessário que tenham determinadas características ou que preencham determinados requisitos para que possamos considerar como responsáveis pelo tratamento.

A grande maioria da prática demonstra que são pessoas coletivas quem assume este papel, o que se entende por serem normalmente pessoas coletivas que tem alguma finalidade e contacto com dados de pessoas e que por isso tem a necessidade de proceder ao tratamento dos seus dados pessoais. As pessoas coletivas podem designar, sempre que assim o entendam, uma pessoa singular que desempenhe funções em seu nome para tratar os dados e aparentar ser ela quem assume a responsabilidade pelo tratamento. É apenas aparentemente, visto que, quem é sempre verdadeiramente responsável é a pessoa coletiva, atuando a pessoa singular apenas como uma forma de personificação do responsável pelo tratamento. Não nos podemos esquecer que estando a desempenhar funções encontra-se sobre as ordens e orientações da entidade para a qual trabalha e apenas se encontra a atuar conforme foi contratada, sendo que tudo o que advém dessas funções pertence e é da responsabilidade do responsável pelo tratamento, não podendo a pessoa coletiva afirmar não ter qualquer responsabilidade pelos atos do seu trabalhador quando este apenas se encontra a cumprir o que lhe foi designado¹⁰⁶.

¹⁰⁵ CORDEIRO, A. Barreto Menezes, - Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, op.cit., página 88.

¹⁰⁶ O artigo 29.º do RGPD qualifica estas pessoas como sendo “qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento”. Não assume em nenhum momento uma responsabilidade conjunta com o responsável pelo tratamento. A responsabilidade é apenas do responsável pelos atos que pratique de acordo com o tratamento e instruções que lhe sejam dadas por ele. Cumprindo as medidas técnicas e organizativas adotadas pelo responsável, como foi mencionado que o deve fazer, e cumprindo as finalidades do tratamento não existe justificação para que seja a pessoa que trabalha para o responsável, assim como o subcontratante, a assumir a responsabilidade pelo tratamento indevido dos dados, como foi já mencionado.

Contudo, é entendido relativamente às funções que desempenhe relativas aos dados pessoais que caso esse trabalhador trate dados para uma finalidade que não lhe foi incumbida assumirá a responsabilidade pelo tratamento desses mesmos dados, não se podendo responsabilizar o responsável por todos os atos que não possa este prever ou assumir.

Por outro lado, não há uma exigência quanto a quem pode ser essa pessoa coletiva, não havendo a indicação de critérios que restrinjam a legitimidade a determinadas pessoas coletivas para o tratamento de dados. Não releva que seja uma autoridade, um organismo ou outra pessoa coletiva que assuma a responsabilidade pelos dados que recolhe sendo apenas exigido que seja quem determine como é que os dados recolhidos serão tratados e protegidos. O que releva não é a natureza jurídica do responsável pelo tratamento nem dentro desta que figura assumem, mas sim aplicarem todas as normas e cumprirem todos os deveres a que estão incumbidos de acordo com as finalidades e meios que definiram na sua constituição como responsável pelo tratamento.

3.2.2.3.3. Responsável de forma individual ou em conjunto com outro responsável

O segundo elemento é o modo como a responsabilidade pode ser assumida, ou seja, a questão de determinar se pode a responsabilidade pelo tratamento ser assumida por mais do que uma pessoa, em conjunto com outro responsável, ou se não podem haver dois ou mais responsáveis pelo tratamento dos mesmos dados. O artigo 26.º consagra de forma direta e sem quaisquer questões interpretativas que a responsabilidade pode ser assumida por um ou mais responsáveis desde que estabeleçam em conjunto as finalidades que vão assumir e de que modo vão proceder ao tratamento dos dados que irão recolher, que medidas técnicas e organizativas vão tomar e de que meios vão dispor para agir em caso de partilha indevida¹⁰⁷. Havendo uma divisão de responsabilidade, impõe o artigo mencionado que haja um ponto em comum que possa permitir deste modo aos titulares exercer os seus direitos e saber como é que o tratamento está a ocorrer. O titular pode sempre, contudo, exercer os seus direitos relativamente a algum dado junto de qualquer um dos responsáveis independentemente do acordo estabelecido para que assim não tenha ainda o inconveniente de se ver limitado a exercer aquilo que entender como necessário sobre os seus dados pessoais.

¹⁰⁷ Podemos através da interpretação da lei e com o apoio das orientações da Comissão entender que em termos de legislação europeia nesta matéria não há uma exigência em concreto dos contornos em que se baseiam os acordos estabelecidos entre os dois responsáveis, mas sim que o façam sempre tendo em conta as mesmas finalidades e as mesmas medidas técnicas e organizativas estabelecidas por si no acordo. As Orientações 07/2020 sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD Versão 2.0 é uma das orientações que permite esta conclusão e pode ser consultada em https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_pt.pdf página 4.

O artigo 26.º na sua primeira parte vem reforçar o que já está consagrado no conceito de responsável pelo tratamento no artigo 4.º não trazendo deste modo nenhum acrescento ao que já era sabido. O modo como é interpretado e entendido o conceito do artigo 26.º tem de ser sempre de modo amplo, visto que, não é um conceito limitativo ao modo como a responsabilidade tem de ser dividida ou como é que deve essa responsabilidade ser perceptível. A responsabilidade tem de ser assumida pelos Estados-Membros de igual modo e de forma coerente de forma a proteger as pessoas singulares o melhor possível e transmitir segurança de que os dados estão protegidos sendo que só isto importa para a União quando criou o RGPD.

Para o titular dos dados não podem existir dúvidas sobre a existência de uma proteção dos seus dados independentemente das características que a mesma assume. Não lhe importa quem assume a responsabilidade, se há mais do que um responsável, se a divisão da responsabilidade no caso de haver mais do que um responsável é feita de modo igual ou não ou a natureza jurídica dos responsáveis. O que importa para o legislador e para o titular dos dados é que haja medidas técnicas e organizativas adotadas adequadas e que a lei seja sempre cumprida quanto à proteção dos dados pessoais independentemente das circunstâncias ou da organização interna do responsável. Os dados pessoais são um bem a proteger independentemente de qualquer outro fator, independentemente como o responsável ou responsáveis se organizam ou dos meios que entendem que são os melhores para tutelar os direitos do titular dos dados. Não tem o titular dos dados se preocupar com quem em concreto procede ao tratamento de um determinado dado seu, qual dos dois responsáveis é que tem essa parte na responsabilidade ou se está perante um subcontratante e não um responsável pelo tratamento. Os interesses e direitos do titular tem de ser sempre considerados e priorizados, em cumprimento do princípio da lealdade, assim como tem de ser sempre tomadas medidas pelos responsáveis de modo a garantir que haja confidencialidade dos dados que o titular partilha, em cumprimento do princípio da confidencialidade.

A responsabilidade conjunta não pode, contudo, ser confundida com a responsabilidade assumida por um subcontratante. Um subcontratante é “uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes”, artigo 4.º, 8) do RGPD, e nesta medida apenas pratica os atos que lhe foram delegados em seu nome e segundo as finalidades e medidas técnicas e organizativas que o responsável designou. Em caso de violação de dados a responsabilidade é

sempre assumida pelo responsável pelo tratamento que delegou os poderes no subcontratante. Através desta breve elucidação, e do que já foi referido, podemos perceber que são conceitos diferentes dado que a responsabilidade conjunta é assumida pelos responsáveis de forma direta e são eles que assumem a responsabilidade e tratam os dados enquanto que os subcontratantes não assumem a responsabilidade e tratam dos dados em nome do responsável. Os responsáveis conjuntos definem como vão atuar e não atuam em nome um do outro, enquanto que o subcontratante não tem interferência do modo como o tratamento é delineado e apenas cumpre do modo como foi contratado pelo responsável.

3.2.2.3.4. Que define as finalidades do seu tratamento de dados e os meios para as concretizar

Quanto a este elemento concretizador do conceito de responsável pelo tratamento já foi sendo dada algumas pistas e menções a seu respeito que nos permitem chegar a este elemento e sabermos/deduzirmos o que significa. O tratamento de dados inicia-se com a definição das finalidades que vão nortear o tratamento de dados e para as quais os dados pessoais vão ser recolhidos e, por outro lado, vão definir quais as medidas técnicas e organizativas que melhor se adequam aos dados e às finalidades e que permitem que haja um cumprimento das obrigações definidas no RGPD para o tratamento de dados. As medidas técnicas e organizativas fazem parte da responsabilidade do responsável pelo tratamento¹⁰⁸ e devem ser as mais adequadas tendo em conta a natureza dos dados recolhidos, as finalidades do tratamento e o circunstancialismo que o tratamento tem de modo a os dados do titular tenham a proteção necessária¹⁰⁹. Por circunstancialismo entende-se que nem todos os dados implicam medidas tão restritas em comparação com outros assim como há dados que, por exemplo, não existem em formato papel e nesse sentido não tem o responsável de adotar medidas relativamente à proteção desses mesmos dados nesse formato.

O responsável pelo tratamento tem de adotar todas as medidas que considere que irão limitar os riscos de uma partilha indevida dos dados, do seu desaparecimento ou modificação, não conseguindo, contudo, nunca prever todas as possibilidades que derivam dos riscos

¹⁰⁸ O artigo 24.º consagra esta responsabilidade dos responsáveis pelo tratamento quanto aos dados pessoais que recolhem ao referir que tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

¹⁰⁹ O Acórdão com o Processo n.º C-293/12 de 8 de abril de 2014, seguindo a diretiva de 95 prevê que Estados devem sempre adotar as medidas que protejam os dados pessoais nas comunicações como meio preventivo e cumpridor da proteção efetiva dos dados dos seus cidadãos, o que vem na linha orientadora das normas europeias.

inevitáveis que a recolha de dados significa para o titular dos mesmos¹¹⁰. Apesar de todos os esforços que o representante possa assumir para cumprir a legislação aplicável nunca poderá garantir com segurança que todos os dados que recolheu não podem ser ameaçados de algum modo. É da sua responsabilidade o cumprimento da legislação aplicável¹¹¹ e nesse sentido são vários os artigos e considerandos que impõe ao responsável um comportamento inquestionável sempre que recolhe dados pessoais e em vários aspetos que compõe o tratamento. Em matéria de pseudonomização, a título de exemplo e no seguimento da sua menção como concretizador do princípio da segurança, consagra o considerando 29 do RGPD, que deve ser permitido ao responsável aplicar as medidas técnicas e organizativas que permitam que o tratamento que desempenhe relativamente aos dados pessoais que recolheu seja dividido de acordo com os dados e permita que determinados dados possam ser assim separados dos outros recolhidos e limitar a possibilidade de identificação do titular dos dados. Assim como o considerando 41 que consagra que devem ser adotadas as medidas necessárias para a transparência e minimização dos dados, que pode ser correlacionada com os princípios da lealdade e da segurança mencionados, e que significam que o responsável terá sempre de zelar pelos dados que recolhe e ser transparente quanto aos riscos e correções necessárias aos dados, por estarem incorretos ou desatualizados, tomando sempre as precauções que os direitos e interesses dos cidadãos assim o impõe.

Esta preocupação com a adoção de todos os meios e mecanismos que reduzam os riscos já existe desde a Diretiva e por isso muito antes de os dados pessoais serem partilhados do modo e rapidez que o são hoje. Como já foi mencionado anteriormente nos dias de hoje as tecnologias assumiram um papel central indiscutível e muito importante em termos de desenvolvimento e com isso passamos a ter a prestação de serviços de modo digital, sem eliminar, contudo, o formato presencial, e aquisição de bens via digital, para além de lojas físicas. Com a digitalização, em continuação com o pensamento exposto no ponto 1, temos uma partilha de dados pessoais muito superior ao que tínhamos no início da existência da primeira legislação em matéria de proteção de dados, Diretiva 95/46/CE, o que exige uma preocupação e exigência superior das medidas técnicas e organizativas que devem ser adotadas de modo a que possamos ter uma diminuição dos riscos àqueles que são inevitáveis e que podem mesmo assim ocorrer. Sem as medidas que os responsáveis preveem e aplicam teríamos um risco de partilhas,

¹¹⁰ A adoção de medidas técnicas e organizativas que se adequem ao tratamento a ser efetuado pelo responsável pelo tratamento segue a imposição do artigo 24.º.

¹¹¹ Artigo 24.º do RGPD.

modificações ou desaparecimento de dados muito superior ao que temos e que traria consequências negativas à confiança que os titulares teriam na adesão a serviços e aquisição de bens a nível digital. Como já foi sendo afluído anteriormente, a evolução da era digital precisa que a sociedade adira e veja neles uma alternativa à realidade tradicional da prestação de serviços e aquisição de bens.

A Administração Pública existe na era digital cada vez mais porque há por parte dos cidadãos a correspondência e adesão positiva à mesma, há a transmissão da confiança de que pode ser-lhes prestado um serviço com as mesmas finalidades e segurança que o formato presencial. Isto só é conseguido, em parte, porque são adotadas as medidas necessárias para que essa confiança exista e cresça na proporção necessária. Assume aqui um papel absolutamente fulcral para o desenvolvimento e atingimento de novas metas em termos de evolução dos serviços e aquisição de bens que como sociedade desejamos atingir e adquirir para que novos níveis de evolução sejam assim assumidos.

O responsável pelo tratamento assume, independentemente de quem seja, um objetivo que só pode ser claro e concreto, a proteção dos dados do titular dos dados que recolhe. As finalidades e meios que adota para o tratamento e para a resolução de eventuais problemas que surgem devem ser o mais claro para o titular. Não podem haver questões quanto ao modo como responsável, ou subcontratante que atua em nome deste, procederá no tratamento dos dados a partir do momento em que os recolhem, tem de estar por ele, responsável, definido para que finalidades estão a recolher os dados, que meios adotaram para o tratamento do mesmo em casos de estes serem partilhados de forma indevida, modificados ou desaparecidos assim como os que adotará para que não isso ocorra. Têm de ter a consciência da responsabilidade que assumem sem puderem alegar que desconheciam as funções que lhes incumbiam, não basta terem as medidas técnicas e organizativas determinadas e previstas se depois não as puserem em prática, praticarem atos relativamente aos dados pessoais que não estão previstos nas finalidades estabelecidas ou não souberem e adotarem os meios que são essenciais para o tratamento dos dados. Tem de haver transparência na sua atuação e clareza de que todos os seus atos têm consequências, sejam elas positivas ou negativas, que podem ser esperadas, inesperadas, reversíveis ou irreversíveis.

3.2.2.3.5. Competências assumidas pelo responsável pelo tratamento

Sabendo quem são os responsáveis pelo tratamento e as linhas básicas da sua atuação enquanto tais, torna-se importante delimitar as competências que irão assumir ou que podem assumir na sua atuação sendo elas a definição das finalidades que irão nortear a sua atuação no tratamento de dados, adoção de meios tratamentos adequados aos dados que recolheu e sob os quais se responsabilizou¹¹² e a nomeação do Encarregado da Proteção de Dados.

3.2.2.3.5.1. Definição das finalidades

O responsável pelo tratamento tem a competência de definir qual ou quais são as finalidades que cada uma das atividades que desempenha, que envolvam dados pessoais, de modo a que o titular dos dados possa saber e ter um conhecimento esclarecido sobre quais os atos que o responsável vai praticar. Estabelecida a finalidade fica deste modo demonstrado que os dados serão tratados para aquele determinado fim e consequentemente é de clara evidência quais os atos que poderão ocorrer. Se o responsável pelo tratamento recolhe a impressão digital para o registo e controlo de trabalho é evidente para o titular, colaborador neste caso, que a finalidade de registo e controlo de tempos de trabalho é a finalidade que motiva a recolha da sua impressão digital.

As finalidades de cada atividade de tratamento atuam como limites/barreiras ao responsável pelo tratamento não podendo este praticar atos que não se encontrem enquadrados com a finalidade que foi comunicada ao titular dos dados. Este tem determinada expectativa e tem o direito de que os seus dados sejam tratados apenas de acordo com aquilo que o responsável se comprometeu quando os recolheu. Estabelece o princípio de limitação de finalidades, consagrado na alínea b) do n.º 1 do artigo 5.º do RGPD, que os dados pessoais são “recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades” e em conjunto com o considerando 60 estabelece que a atuação do responsável para que seja transparente e equitativa tem de ser sempre de acordo com as finalidades que ele próprio delimitou. Como é que o princípio da segurança, ou princípio da transparência, pode ser cumprido se o titular não puder na verdade contar com todas as informações reais e verdadeiras sobre o tratamento dos seus dados, se a finalidade que lhe foi informada pelo responsável já não é a mesma que inicialmente prestada? Como foi desenvolvido previamente a atuação em matéria de proteção de dados tem de ser

¹¹² No conceito de responsável pelo tratamento previsto no artigo 4.º, 7) do RGPD é estabelecido estas duas competências.

sempre transparente e clara para o titular dos dados quer quanto aos atos, quer quanto aos meios quer quanto ao modo como o tratamento vai ser efetuado. As finalidades do tratamento fazem logicamente parte dos elementos a ser conhecidos pelo titular¹¹³ de modo a que possa exercer os seus direitos sempre que entender e para que não seja surpreendido com o tratamento dos seus dados para uma finalidade que não concorda e para a qual não consentiu, quando o consentimento é o fundamento, ou segundo a qual não formou a sua vontade em partilhar os seus dados.

O consentimento, um dos fundamentos de licitude mencionado anteriormente, é, como já se constatou, um fundamento exigente e frágil porque basta que não seja completamente claro e delimitado o seu âmbito para que não possa ser fundamento de licitude. Se o consentimento é prestado de acordo com determinadas finalidades basta que estas não correspondam à realidade para que estejamos perante um caso de tratamento ilícito de dados. É esta a importância da transparência das finalidades e do cumprimento rigoroso dessas finalidades. Não existem casos em que se compreende que o responsável possa não estar consciente que os atos que praticou durante o tratamento se estão a afastar ou que não se enquadram com as finalidades que estabeleceu por serem atos que parecem estar conforme essas finalidades, o responsável pelo tratamento tem que ter sempre consciência dos seus atos.

Os direitos que estão previstos a partir do artigo 15.º do RGPD são reconhecidos ao titular e podem ser exercidos se a atuação do tratamento não corresponder com as finalidades que estabeleceu. Por exemplo o direito de acesso, artigo 15.º, reconhece ao titular o direito de aceder aos dados que foram recolhidos pelo responsável e de saber quais são as finalidades em que os seus dados estão a ser utilizados. As informações prestadas nesta matéria têm de corresponder à verdade e não podem desviar-se dela e o titular dos dados deve ter a possibilidade de reagir relativamente a qualquer desconformidade.

3.2.2.3.5.2. Meios de tratamento

O responsável pelo tratamento tem de prever ainda como é que os titulares dos dados poderão exercer os seus direitos, previsto no artigo 15.º do RGPD e seguintes, sempre que o entendam fazer. O modo de exercício de direitos poderá ser feito através de email ou de modo presencial através do preenchimento de um formulário. Havendo a decisão de permitir que o exercício de direitos ocorra por email há a necessidade de consagrar um meio de fazer

¹¹³ Considerando 63 do RGPD.

presencialmente visto que nem todas as pessoas tem email. O titular não pode sentir dificuldades em exercer os seus direitos sempre que assim o entender. Os meios de tratamento são pensados, como se pode perceber, sempre no titular.

3.2.2.3.6. Obrigações do responsável pelo tratamento de acordo com as suas competências

Uma das principais obrigações do responsável pelo tratamento é que permite que, em caso de partilha indevida, possam ser adotadas medidas de proteção mais concretas que protejam e minimizem os prejuízos que podem ter ocorrido com a partilha dos dados de forma indevida e por outro lado demonstra a magnitude da partilha, é o Registo de Atividades de Tratamento (RAT)¹¹⁴. Os responsáveis pelo tratamento devem ter sempre atualizado este registo que consiste numa síntese que permite perceber como é que os dados circulam dentro da organização do responsável pelo tratamento, quer através da descrição de como é que circulam quer que meios informáticos e de arquivo são usados, e que em caso de partilha indevida dos dados permite perceber que dados foram comprometidos e possíveis lacunas que possibilitaram a partilha. Se a partilha se verificar, a título de exemplo, no Departamento dos Recursos Humanos de uma entidade é possível perceber com quem partilham os dados, que aplicações informáticas usam e como é o arquivo dos documentos que contém dados pessoais. O conhecimento integral do percurso dos dados pessoais e o modo como estes são conservados é a chave essencial para que se possa adotar medidas que diminuam os danos que se verificaram com a partilha indevida dos mesmos. Sem um RAT atualizado não se tem num primeiro instante e de modo rápido, e talvez nunca se terá, uma perceção da realidade dos danos que foram causados e de quais são os melhores atos a ser praticados pelo responsável em resposta ao incidente. Estamos a falar, como já foi mencionado mais do que uma vez anteriormente, de dados de extrema importância para o titular e que só com o comportamento correto e adequado é que os direitos e interesses do titular dos dados podem ser salvaguardados e acautelados outros possíveis danos que podem eventualmente surgir. O subcontratante¹¹⁵ tem que ter o seu registo relativamente às atividades que desempenham em nome do responsável de modo a que possa cooperar com este em caso de incidentes relacionados com dados que tem acesso no exercício das suas atividades como subcontratante. Esta obrigação¹¹⁶, contudo, é apenas para responsáveis pelo tratamento de

¹¹⁴ O artigo 30.º do RGPD consagra no seu n.º 1 a obrigação de o responsável elaborar e conservar o registo de todas as atividades que desempenha que contenham dados pessoais e todas as informações relativas ao modo como desempenha essas atividades.

¹¹⁵ O n.º 2 do artigo 30.º do RGPD consagra a responsabilidade do subcontratante em matéria de registo das atividades de tratamento que pratica em nome do responsável.

¹¹⁶ N.º 5 do artigo 30.º do RGPD.

entidades com mais de 250 trabalhadores¹¹⁷, quando a atividade desempenhada possa pôr em causa direitos e liberdades do titular dos dados, quando não seja ocasional, quando estejam em causa categorias especiais de dados ou ainda quando estamos perante dados pessoais relativos a condenações penais e infrações. As autoridades de controlo requerem este registo, nos casos aplicáveis, de modo a que possam perceber como é que houve dados divulgados indevidamente, que dados é que foram e a verdadeira extensão da violação de dados ocorrida.

Esta obrigação é de alguma forma um meio de orientação para os responsáveis pelo tratamento de modo a saberem sempre como agir e cumprir as normas legais com mais facilidade e com mais rapidez de atuação nos casos necessários. Ao ter mais de 250 trabalhadores estamos a falar de entidades com um volume de dados considerável e consequentemente maior será a dificuldade de tratamento de dados quanto maior for o número de dados que recolhem. A organização de como o tratamento é efetuado e sobre que atividades é feito pode ser o primeiro passo para que a minimização dos riscos, a minimização dos dados recolhidos e a minimização dos efeitos negativos para os direitos e interesses do titular sejam minimizados. A perceção do caminho que os dados percorrem e que atividades são praticadas pelo responsável e sob a justificação de determinadas finalidades é a representação de uma atuação conforme e de acordo com o principal foco no tratamento dos dados: o titular dos dados. Os problemas que possam existir no tratamento de dados e que potenciam determinados problemas, confusões ou menor eficiência podem advir e ser corrigidos ou minimizados caso haja uma organização num único registo das atividades que são desenvolvidas e de como estas ocorrem na prática.

Uma outra obrigação que é da competência do responsável pelo tratamento de dados e que ajuda na concretização dos objetivos mencionados com a existência do RAT é a realização de Avaliação de Impacto do Tratamento de Dados (AIPD)¹¹⁸. A obrigação de serem feitas avaliações de impacto decorre do artigo 35.º do RGPD e existe sempre que, devido aos elevados riscos que uma atividade de tratamento representa para os dados pessoais, seja prudente o responsável pelo tratamento perceber qual o impacto que aquela atividade terá para os dados recolhidos. É uma ferramenta que deve e que tem de ser usada pelo responsável antes de iniciar a atividade e não no decorrer da mesma. A avaliação feita durante o tratamento, para além de incorrer num

¹¹⁷ A CNPD não concorda com a limitação desta obrigação aos responsáveis com mais de 250 trabalhadores, visto que, entende que todos os responsáveis pelo tratamento devem ter um registo das atividades de tratamento (RAT) que desempenham independentemente do seu número de trabalhadores. O RAT é muito útil para todos os responsáveis pelo tratamento em caso de violações de dados.

¹¹⁸ Considerando 80 do RGPD.

incumprimento legal, pode representar que o(s) impacto(s) negativo(s) que se quer evitar pode já não ser possível de se fazer. o impacto que se pretende avaliar é aquele que se não se quer que se verifique e que venha a causar mais desvantagens do que vantagens para o tratamento dos dados pessoais. A avaliação é feita pelo encarregado pela proteção de dados¹¹⁹, se tiver sido designado, ou por outra pessoa com essas competências, ou pelo próprio responsável pelo tratamento. Estas avaliações são mais significativas quando meios informáticos são usados para o desempenho de atividades pelo responsável pelo tratamento ou pelo subcontratante e que por serem meios que, teoricamente, representam mais riscos e mais probabilidade de tratamento ilícito dos dados e, por outro lado, são dados que permitem com muita facilidade identificar o titular dos dados. O uso de câmaras de vigilância ou o uso de geolocalização de veículos de uma empresa são dois exemplos de atividades que precisam que seja feita uma AIPD para que se possa perceber qual o impacto que a atividade terá para o titular dos dados. Compreende-se esta abordagem e esta perceção de que há atividades que representam e impõe um comportamento preventivo ativo por parte de quem recolhe os dados pessoais, só assim podem os titulares confiar os dados e perceber que estes estão salvaguardados, e como forma de prevenir que seja responsabilizado por riscos que podiam ser minimizados e alguns evitáveis. Os riscos não deixam de existir, mas há mecanismos como estes dois que permitem que a probabilidade de ocorrerem seja diminuída ou que caso ocorram, no caso do RAT, sejam uma forma de diminuir os efeitos negativos.

Estas duas obrigações são igualmente essenciais para o exercício de funções pela Administração Pública, à medida que caminhamos para uma administração aberta, princípio da administração aberta, como responsável pelo tratamento. A administração aberta onde os dados circulam com uma maior facilidade só pode ser possível se houve um registo de todas atividades que são desempenhadas ao pormenor, com toda a correspondência com a verdade e com a avaliação dos casos em que pode haver um impacto negativo mais significativo com um determinado tratamento. A Administração Pública não pode permitir que os dados circulem quer nacionalmente quer em conexão com a União Europeia se não tiver consciência e perceção do que a mesma significa para o universo de titulares de dados que abrange. A circulação de dados significa um progresso benéfico para a sociedade e representa a concretização da ideia de que

¹¹⁹ O encarregado pela proteção de dados nem sempre tem de ser designado pelo responsável pelo tratamento. O artigo 37.º prevê os casos em que pode o responsável pelo tratamento designar estando nos artigos seguintes a consagração das suas funções e da sua relação com o responsável pelo tratamento e com o(s) subcontratante(s) caso exista. Contudo, há casos, previstos no n.º 1 do artigo 37.º em que é obrigatório que o responsável pelo tratamento e o subcontratante designem um encarregado.

a sociedade deve evoluir, adaptar-se e querer sempre mais para que se consiga sempre melhorar hoje aspetos do passado, mas com isso não pode significar uma evolução a todo o custo. Os tempos mudam e evoluem e a necessidade de haver novas conquistas, novos meios e serviços melhores é evidente, inegável e necessária para que os problemas do passado sejam resolvidos e para que os problemas que existam hoje possam ter uma solução no futuro, é inegável, mas tudo tem o seu custo e este tem que ser acautelado sempre. Um serviço que pode ser prestado por mais do que uma entidade, que comunicam dados entre si sem que o titular tenha de o fazer sempre que se dirige ao mesmo, só beneficia todos, o serviço e o titular. O serviço torna-se mais rápido e prestativo dos interesses do titular e consegue ele próprio evoluir e ao mesmo tempo o titular consegue ver os seus interesses a cumprirem-se com mais rapidez, menos burocracia e com isso menos problemas para o titular. Há deste modo uma comunicação e ligação maior entre os serviços e entre estes e os cidadãos que visam, contudo sem que signifique ao mesmo tempo que estamos a concordar pôr em causa direitos fundamentais em nome de uma evolução. A evolução tecnológica pode esperar se isso significar proteger os cidadãos e permitir que os benefícios sejam sempre superiores às desvantagens. A renovação do cartão de cidadãos, a título de exemplo, sem ter de haver uma deslocação, com possível perda de parte do seu horário de trabalho e consequentemente remuneração, puder ser feita com segurança dos dados que introduzimos no sistema online é de facto benéfico para o cidadão. Num outro prisma estes benefícios deixam de existir se com eles houver uma violação de dados para o titular e consequentemente passam a significar um inconveniente que o mesmo ato praticado da forma tradicional tem maior dificuldade em ocorrer. Não nos podemos esquecer ao mesmo tempo que esta evolução não pode, contudo, eliminar os meios e os serviços físicos, uma pessoa sem os meios informáticos necessários tem de ter sempre a possibilidade de os serviços lhe serem prestados. A prestação de serviços de modo presencial ou online tem de ser para o cidadão duas formas iguais em termos de qualidade, representando assim verdadeiras alternativas.

3.3. Responsabilização em caso de violação de dados

A questão que se coloca é saber se é sempre de fácil determinação quem assume a figura de responsável pelo tratamento, de quem verdadeiramente assume a responsabilidade quando ocorre uma violação de dados. Será a lei suficientemente clara sobre quem deve assumir a responsabilidade em todos os casos de incidentes ou ainda haverá casos concretos em que quem deve assumir a responsabilidade é pouco claro? A determinação de quem é o responsável pelo tratamento não é em todos os casos preto no branco, havendo determinados casos em que

os elementos práticos do caso nos colocam a dúvida. Por outro lado, o controlo que é feito sobre os atos praticados pelo responsável pelo tratamento, e que determinam que haja a necessidade de haver uma alteração do tratamento, tem sido encarado de modo diferente pelo legislador. Estas modificações derivam do que a realidade revela como necessário para que possa haver uma legislação de acordo com aquilo que faz sentido para as dificuldades que existem no dia-a-dia e que tem que ser combatidas através de alterações legislativas.

Atualmente o modelo de controlo dos responsáveis pelo tratamento é a autorregulação do tratamento de dados desempenhado pelo responsável pelo tratamento, entendendo-se que não há uma necessidade de haver um controlo prévio dos atos praticados por aquele e que caso haja a necessidade de agir ocorrerá posteriormente. Entende-se segundo este modelo que o controlo prévio dos atos que o responsável pelo tratamento entender praticar e que possam ter um impacto nos dados pessoais não é de seguir dado os inconvenientes temporais. O controlo prévio dos responsáveis, a heterorregulação, pode parecer mais protetivo para os dados dos titulares, pelo modo como são atenuados os efeitos e probabilidade das violações de dados e das medidas que são adotadas para que o tratamento de dados seja feito de acordo com os parâmetros que melhor se adequam ao cumprimento legal e para que o impacto que um determinado ato possa ter possa ser amenizado ou impedido de ser praticado esse ato. São diversos os fundamentos que existem para que exista quer uma autorregulação quer uma heterorregulação, mas o que importa aqui é saber qual dos dois modelos é o mais eficaz, quer em termos substantivos em matéria de atos a ser praticados, quer em termos temporais, demora na tomada de decisões, para que a probabilidade de ocorrência de uma violação de dados possa ser o mais diminuída possível. Nem sempre houve o mesmo entendimento, mas tudo tem relação com o que está a acontecer na realidade digital e com as necessidades de o legislador agir em conformidade com o que vai beneficiar mais a atuação do responsável pelo tratamento e no que pode ser exigível para que a digitalização não seja limitada.

3.3.1. Principais modificações legislativas entre 1995 e 2018 – o impacto na perceção da regulação de heterorregulação a heterorregulação mitigada?

A legislação em matéria de proteção de dados foi evoluindo ao longo do tempo de acordo com o que foi sendo entendido como necessário para acompanhar a evolução digital, com o aumento do número de dados que circulam e com a existência de mais responsáveis pelo tratamento. O entendimento sobre a realidade digital foi modificando e foi sendo claro que era

necessário reconhecer autonomia aos responsáveis pelo tratamento pelos dados no que toca ao tratamento dos dados se queríamos que a digitalização não se tornasse numa tarefa demasiado penosa e pesada.

Nos primeiros anos de digitalização foi consagrado que a heterorregulação dos responsáveis pelo tratamento permitia que houvesse um maior controlo e uma ação mais ponderada e com um maior conhecimento sobre quais os atos que tinham que ser praticados e que medidas técnicas e organizativas tinham que ser adotadas para que a tutela dos dados pessoais fosse a melhor que poderia existir. O conhecimento técnico era pouco dada a novidade do tema e a dificuldade de saberem determinar num caso concreto como haveriam de agir para que o tratamento de dados que determinaram ou os atos que queriam praticar não fossem mais prejudiciais do que benéficos para aqueles que queriam beneficiar, os titulares dos dados. Foi assim que o legislador entendeu quando analisou os riscos que um serviço público digital representava e como deveria agir para que fizesse aquilo que permitisse uma atuação adequada e que levasse à existência da confiança necessária na partilha de dados não deixasse rapidamente de existir por falta de benefícios que justificassem os riscos que estavam a ser criados. Não podíamos esperar que houvesse um cenário diferente por parte de quem tem que tomar decisões sobre o seu serviço ou entidade dado que não há conhecimento que se adquira sem que a prática exista, sem prática não há evolução, mas há ao mesmo tempo erros que podem ser demasiado prejudiciais e que podem ser evitados, entendiam assim, com um controlo prévio que funcionava como cooperação para com o responsável.

3.3.1.1. Diretiva 95/46/CE

A Diretiva 95/46/CE¹²⁰ surge como diploma sucessor à Convenção 108 do Conselho da Europa de 1981, por sua vez, surgindo depois de duas resoluções aprovadas em 1973 e 1974 relativas à proteção da privacidade das pessoas singulares perante os bancos eletrónicos de dados no setor público e no setor privado, respetivamente, criada com o objetivo de regular a matéria da proteção de dados numa fase embrionária da digitalização dos dados, circulação e tratamento dos mesmos e, como já foi mencionada anteriormente, de uma importância

¹²⁰ A Lei n.º 67/98, de 26 de outubro foi a lei portuguesa que transpôs a Diretiva 95/46/CE e que marcou a evolução legislativa em matéria de proteção de dados. A nossa Constituição já previa esta matéria no seu artigo 35.º, contudo, não era, de forma evidente, suficiente para regular uma matéria tão vasta e em claro crescimento. A Diretiva veio permitir que, através da sua transposição pela lei mencionada, houvesse em conjunto com a CRP uma regulação da matéria de acordo com o que eram as necessidades na época e do que era necessário para que pudesse haver uma evolução dessas mesmas necessidades.

descomedida. A Convenção 108 foi criada pelo Conselho da Europa como resposta às alterações que foram sendo verificadas no campo da proteção de dados e a proteção das pessoas relativamente às decisões automáticas que recaiam sobre si. Era evidente que as partes que faziam parte da Convenção teriam de adotar medidas que tivessem em conta os titulares dos dados e não apenas os seus interesses de evolução tecnológica e de negócios e nesse sentido é que foi elaborada. A noção de dados pessoais ganhou importância e começou a ser entendido o seu verdadeiro significado e dimensão e que preocupações deveriam ser assumidas por quem os recolhia e os tratava de acordo com determinada(s) finalidade(s). Houve a determinação de princípios que visavam a qualidade e segurança dos dados em qualquer circunstância do uso dos mesmos, assim como, a determinação de um regime especial para os dados sensíveis, que precisam de uma proteção mais fortificada, e, por outro lado, a definição de um conjunto de garantias reconhecidas ao titular dos dados de forma a que possa ter meios que o ajudem a controlar as finalidades para as quais os seus dados são utilizados. Foram passos essenciais que significaram o alcance de novas metas tecnológicas e principalmente impulsionou os primeiros a evolução legislativa em matéria de proteção de dados à medida que tentava acompanhar os efeitos que podiam derivar dessa evolução.

A Diretiva surgiu como um instrumento de uniformização das legislações nacionais, que previam normas sobre a proteção de dados, mas muito centrados no seu Estado, de modo a direcioná-las para uma perspetiva europeia e consequentemente possibilitar que a vontade de criar uma comunicação e transmissão de dados entre os Estados e entre estes e a UE em prol dos cidadãos europeus fosse convenientemente regularizada. Se a ideia era que os Estados comunicassem entre si dados no sentido de promover a prestação de serviços a todos os cidadãos europeus e que todos os países estivessem ao mesmo nível no alcance da circulação de dados então tornou-se essencial perceber a urgência de criar um instrumento legislativo capaz de garantir que essa vontade era possível ser feita de uma forma cautelosa e com o alcance que se pretendia. A resolução de casos concretos, a exigência de princípios aplicáveis e meios de proteção dos titulares dos dados tornaram esta Diretiva a principal responsável pela viragem na direção certa do que se entendia dever ser o trajeto a seguir por todos os aplicantes de direito, políticos, economistas, entre outros, sempre que recorrem a métodos e meios digitais para cumprir com os seus objetivos. A Diretiva veio responder a todos os pedidos de intervenção legislativa para que houvesse o reconhecimento pelo legislador das alterações que se estavam a verificar e que exigiam uma evolução em nome da proteção dos dados pessoais e dos titulares

dos dados. A evolução só pode existir se houver uma proteção adequada e justa às características e realidade da mesma dos direitos reconhecidos aos cidadãos e se for possível que haja uma justiça digitalizada que beneficie a sua aplicabilidade e não se torne apenas um instrumento criado com poucos efeitos práticos. Com uma legislação adequada os cidadãos beneficiam com uma proteção jurídica que vai de encontro aos seus interesses, evolutivos, e com uma maior capacidade judicial de resposta aos problemas que se colocam e que os meios judiciais passam a conseguir corresponder.

Para além do âmbito pessoal, dos cidadãos, outros aspetos importantes que eram desejáveis com a digitalização como a transmissão de dados entre os Estados-Membros revelaram-se um lapso na Convenção de 1981 por não se ter previsto que os Estados não se encontravam no mesmo patamar de evolução e desenvolvimento quer em termos legislativos e regulamentares quer em termos administrativos e nessa medida legislativamente era preciso ter isso em consideração. Não podemos reagir contra um Estado e aplicar uma coima ao mesmo pelo incumprimento da lei se não tivesse condições de o fazer de uma forma imediata assim como os outros Estados mais desenvolvidos e com maior capacidade de resposta quer em termos económicos quer em termos de meios. Os responsáveis da União constaram que a transmissão desejada em prol da unificação da União só seria possível se houvesse uma diferenciação dos Estados de acordo com o seu nível de digitalização e meios e com o reconhecimento que os timings de resposta de cada um era diferente. Iniciou-se uma “ação comunitária com vista à aproximação de legislações”¹²¹ e que se concretizou na Diretiva 95/46/CE. Esta diretiva destacou-se pela sua determinação de meios, princípios e limites que permitiram que a matéria da proteção de dados reunisse todos os ingredientes para transmitir a confiança que começava a existir face à incapacidade, por ser incompleta, da convenção mencionada, permitindo deste modo que novas metas fossem alcançadas.

A Diretiva, contudo, foi revelando que eventualmente precisaria de ser reformada quanto ao sistema de controlo dos atos praticados no tratamento dos dados pessoais por parte do responsável pelo tratamento que fossem parcialmente ou totalmente automatizados. Todos os atos que eram praticados pelo responsável pelo tratamento com recurso a sistemas ou softwares informáticos e que permitiam que houvesse a substituição de determinados atos por máquinas

¹²¹ Os primeiros considerandos da Diretiva refletem esta preocupação com a diferença entre os Estados e de que modo uma legislação que a desconsidere não está a cumprir o seu propósito. Os titulares dos dados não conseguem ver os seus dados protegidos e os seus direitos e interesses respeitados se a União prevê uma lei que não tem isso em conta. A União não consegue evoluir se não tiver em conta as circunstâncias dos seus Estados. Funciona tudo como um todo, como uma interligação.

tinham de ser notificados à autoridade de controlo e em alguns casos mais complexos, em que os direitos fundamentais poderiam estar em causa, era necessário que houvesse uma autorização administrativa para que pudessem ser praticados. Para a Diretiva não interessava se eram norteados pela(s) finalidade(s) assumidas e pelos meios que fossem considerados adequados para os dados em causa, de acordo com a definição prevista na alínea d) do artigo 2.º, mas sim por quem eram praticados todos os atos que compunham um determinado tratamento de dados¹²². Este regime revelou a necessidade de ser reformado pela circunstância de se ter tornado evidente a saturação do sistema na capacidade de resposta aos pedidos de autorização que os responsáveis tinham de fazer sempre que queriam iniciar o tratamento ou conjunto atos de tratamentos, total ou parcialmente automatizados, que se relacionavam com a finalidade ou finalidades prosseguidas e interligadas¹²³. Não havia a determinação de exceções para atos que apenas fossem em parte automatizados, havendo apenas critérios que definiam a delimitação dos atos que exigiam que houvesse apenas notificação daqueles em que era preciso uma autorização das autoridades de controlo. A autoridade de controlo de cada Estado tinha deste modo uma responsabilidade e trabalho de uma dimensão incontrolável e que continuamente ficava mais acentuada com a evolução do mundo digital e com a maior necessidade de haver autorizações para proceder a um número cada vez maior de tratamentos de dados. Havia deste modo uma dependência excessiva, que se tornou insustentável, numa única autoridade, visto que a maioria dos Estados apenas tinha uma, para cada vez mais responsáveis pelo tratamento e de dados partilhados e consequentemente uma maior necessidade de ter meios informáticos que permitissem que houvesse uma capacidade de resposta na janela temporal adequada às necessidades dos titulares dos dados.

Esta exigência de autorização deriva do sistema que havia quanto à proteção dos dados na era da Diretiva: a heterorregulação da proteção dos dados pessoais. A regulação dos atos automatizados, total ou parcialmente, praticados pelo responsável era completamente determinada por outrem, que não o responsável, não permitindo ser este a tomar qualquer decisão relativamente a estes atos no âmbito da sua atividade profissional. A regulação vinha de outrem quer quanto à possibilidade de haver um determinado tratamento, como este deveria ocorrer e como deveriam determinar recursos para o exercício de direitos por parte dos titulares

¹²² Os artigos 18.º a 21.º da Diretiva consagravam as obrigações que as autoridades de controlo nacionais tinham na regulação das atividades de tratamento que eram desempenhadas pelos responsáveis pelo tratamento dos seus Estados-Membros. Os atos tinham que ser notificados à autoridade e posteriormente controlados de modo a que pudessem ser praticados.

¹²³ Artigo 18.º n.º 1 da Diretiva 95/46/CE.

dos dados. Havia a denominação das entidades que recolhiam os dados como responsáveis, mas na realidade eram apenas a face que respondia ou lidava com o titular dos dados na primeira linha de contacto e que compreendia que tinha de adotar outros atos que lhe permitissem corresponder às necessidades dos seus principais interessados. Transmitia a ideia de que os responsáveis não podiam ser competentes para a tomada de tais decisões sobre os dados pessoais e o seu tratamento¹²⁴ e que não conseguiam medir os riscos que a utilização de software poderia significar para os dados que estavam a recolher. Estes mesmos responsáveis já eram vistos como capazes para todos os atos que não envolvessem o uso de tecnologias e que fossem totalmente praticados por pessoas.

Foram surgindo demonstrações que a mudança de regime tinha de ocorrer através da recolha de um vasto processo de consulta que a Comissão Europeia criou em 2009 de forma a entender quais as frustrações que existiam e quais as normas que precisavam de ser alteradas. A reforma chegou em 2016 com o Regulamento (UE) n.º 679/2016, de 27 de abril.

3.3.1.2. Regulamento (UE) n.º 679/2016, de 27 de abril

O Regulamento (UE) n.º 679/2016, de 27 de abril marcou a mudança de um sistema de heterorregulação para um sistema de autorregulação como resposta à necessidade de haver uma mudança do momento do controlo por parte da autoridade de controlo. Com o processo de consulta iniciado e realizado pela Comissão Europeia foi claro que teria de haver mudanças no modo como a responsabilidade dos atos automatizados era assumida e qual o papel que os responsáveis pelo tratamento e as autoridades de controlo assumiam nas decisões a ser tomadas quanto ao tratamento de dados mais protetor do direito fundamental de proteção da vida privada dos titulares dos dados. Não poderia haver uma evolução como a que estava a ocorrer havendo uma dependência da dimensão que havia, era um contrassenso querer que os responsáveis pelo tratamento assumissem a responsabilidade pelos seus atos, mas ao mesmo tempo considerar-se que não tem capacidade para praticar atos automatizados sozinhos. O Parlamento Europeu e o Conselho com a criação deste Regulamento entenderam que as normas em matéria de responsabilidade e controlo não poderiam limitar o funcionamento da proteção de dados e nesse sentido os responsáveis pelo tratamento teriam de assumir a responsabilidade na generalidade dos atos que praticassem e só seriam controlados em determinados casos ou

¹²⁴ ALVES, Joel A. – *O novo modelo de proteção de dados de dados pessoais europeu*, Coimbra, Almedina, 2021, páginas 87 a 89.

depois de estes serem praticados caso assim fosse entendido como o melhor para a proteção dos dados.

O controlo administrativo prévio relativamente a qualquer ato que seja praticado pelo responsável pelo tratamento apenas tem que cumprir a exigência de controlo pela autoridade de controlo em dois casos específicos, sendo eles, por um lado quando ocorre uma transferência de dados para países terceiros ou para organizações internacionais que não se encontram dentro da UE¹²⁵, no caso de existir uma decisão da Comissão ao abrigo do artigo 45.º do RGPD que indique que não há um cumprimento das exigências necessárias em matéria de dados pessoais por um determinado país, território ou setores específicos deles e nesse sentido seja necessário salvaguardar os direitos fundamentais dos titulares ou no caso não haja garantias adequadas em termos de cláusulas contratuais ou de disposições específicas a contemplar em acórdãos interadministrativos¹²⁶, por outro lado temos os casos em que é feita uma avaliação de impacto, no âmbito da previsão do artigo 35.º, de uma atividade de tratamento que se pretende implementar e que ao ser efetuada pelo responsável pelo tratamento se entenda que há riscos considerados como elevados para o titular dos dados e que os seus direitos fundamentais podem não estar protegidos se não forem adotadas medidas técnicas e organizativas adequadas para a prevenção desses riscos¹²⁷.

Com a mudança da heterorregulação para autorregulação houve uma diminuição do número de casos que precisavam de notificação ou autorização prévia e equitativamente o número de casos que as autoridades de controlo tinham de decidir neste sentido. Os responsáveis pelo tratamento adquiriram mais responsabilidade com o RGPD o que, por outro lado, veio também significar uma compensação ou até mesmo um aumentar da demora na tomada de decisões quer em termos temporais quer na demanda de todos os atos terem de respeitar um conjunto de obrigações¹²⁸. O princípio da responsabilidade do artigo 24.º é um dos reflexos desta maior responsabilidade do responsável ao impor que todas as medidas técnicas e organizativas devam ser adotadas não só para cumprirem o RGPD, mas também para que caso seja necessário

¹²⁵ Este controlo tem que existir dado que não é possível haver um controlo por parte do Estado ou por parte da UE relativamente aos dados que são transferidos e tratados fora da legislação europeia. Não podemos transferir dados para os EUA e posteriormente querer que a nossa autoridade controle o modo como os dados vão ser protegidos. Ocorre assim um controlo antes com vista a tentar evitar que haja uma partilha de dados para quem não irá assumir nenhuma norma ou poucas normas que protejam os dados de acordo com o seu conteúdo.

¹²⁶ Artigo 46.º n.º 2 alíneas c) e d) do RGPD.

¹²⁷ N.º 1 do artigo 36.º do RGPD.

¹²⁸ O Grupo de Trabalho do Artigo 29.º veio também afirmar que esta diminuição de encargos administrativos e financeiros para os responsáveis não significou que houve uma simplificação do que tem que ser feito por parte do responsável pelo tratamento sempre que inicia uma nova atividade de tratamento. As obrigações que agora são do responsável impõe que haja uma dedicação que pode levar a uma demora na tomada de decisões.

tenham os meios para a autoridade de controlo perceber que adotaram todas as medidas que poderiam esperar ser adotadas em consciência com os dados que recolhem, os riscos que existem e o tratamento mais adequado para esses mesmos dados e riscos¹²⁹. Há um assumir do papel de gestores de responsabilidade, e não apenas responsáveis pelo tratamento que são dependentes da autoridade de controlo, um papel mais relevante no tratamento dos dados pessoais e fazem-no assumindo a “linha da frente” dos problemas que podem existir e a atribuição da culpa por um comportamento que deveriam ter tido e não tiveram quando utilizam meios informáticos para a prática da sua atividade.

Esta modificação do modo de compreender quais as reais necessidades que a realidade digital precisa e de que modo devem ser perspectivadas as normas no sentido de as concretizar resulta do facto de se ter percebido que havendo um controlo prévio necessário para que os atos automatizados pudessem ser adotados era na verdade uma limitação a uma liberdade de circulação que se pretende adotar. Se queremos um Mercado Único Europeu onde a liberdade seja um dos seus principais motores ou se por outro lado queremos que a economia e as pessoas sintam a liberdade de conseguirem circular na UE com a maior liberdade possível não podemos querer que haja uma barreira de autorizações que limite a velocidade que a vida impõe. Um determinado negócio que queira vingar na Europa não pode ter que esperar que haja um controlo administrativo prévio ou que tenha de elaborar uma notificação para que possa substituir certos atos que pratica no seu exercício por programas e softwares que lhe permitem uma gestão de negócio muito melhor¹³⁰. Para além do tempo que se despendia com estas obrigações é de referir de igual modo os custos que as mesmas implicavam para o responsável pelo tratamento e que levavam a que para além do tempo despendido houvesse uma imposição monetária que poderia limitar a prática de novas atividades de tratamento.

Houve de igual modo a substituição de autores de determinados atos nomeadamente os registos de atividades de tratamento passaram a ser elaborados pelos responsáveis pelo

¹²⁹ O considerando 123 do RGPD e o artigo 57.º atuam em conjunto com a delimitação da nova realidade das autoridades de controlo e provam que houve verdadeiramente uma reforma do sistema, há muito esperada e que se reflete na prática. As responsabilidades que passaram a assumir são mais de garantia de que o RGPD é cumprido e não na interferência dos atos que são praticados. O considerando 123 do RGPD é o melhor sumário do que as autoridades de controlo assumem com a mudança para um sistema de autorregulação, ou seja, a mudança de perspetiva adotada quanto ao que deve ser encarado o papel das autoridades de controlo. O artigo 57.º do RGPD vai na mesma linha com a distinção em vários poderes do que pode e é a atividade de atuação das autoridades de controlo. A sua atuação é mais eficiente dada a diminuição da sobrecarga que tinham com a heterorregulação.

¹³⁰ Este alerta do impacto que a eliminação do controlo administrativo prévio pode ter na liberdade dos cidadãos europeus foi feito por Filipa Urbano Calvão no seu artigo “O modelo de supervisão de tratamentos de dados pessoais na União Europeia: Da atual diretiva ao futuro regulamento”.

tratamento e não pelas autoridades de controlo¹³¹. Cada responsável deve ter registado, como foi mencionado anteriormente, todas as suas atividades de tratamento de modo a que caso haja um incidente haja um conhecimento de todas as atividades e do modo como os dados circulam. As autoridades de controlo assumem agora apenas um papel de conhecedores destes registos de modo a cooperar com o responsável pelo tratamento quanto ao que devem fazer no caso de haver um incidente ou caso considerem que é necessário conhecer a atividade do responsável pelo tratamento.

3.3.1.3. Heterorregulação mitigada

O tratamento dos dados pessoais e a responsabilidade que dele deriva nem sempre é uma delimitação que possa ser entendida e posta em prática de uma forma não problemática e sem questões sobre como deve um determinado caso ser resolvido ou quem é que assumirá a responsabilidade em caso de partilha indevida pelos atos praticados ou pelas medidas de técnicas e organizativas não adequadas ao tratamento de dados. O RGPD é claro nas regras que determina para o tratamento de dados e como os responsáveis pelo tratamento devem atuar de forma a cumprir com os princípios aplicáveis à proteção dos dados pessoais. Contudo, tem que ser referido que existem determinadas normas que criam “zonas cinzentas” quanto a quem tem que permitir e assumir a responsabilidade inicial quanto ao controlo de determinados atos.

A responsabilidade que existe nesta matéria é inegável e tem que haver sempre quem a assuma adotando todas as medidas que possam minimizar as violações de dados que podem existir e com as quais é necessário ter em conta e esperar que ocorram quando são requeridos e recolhidos dados de uma determinada pessoa. Com o RGPD, como vimos, houve uma passagem de obrigações das autoridades de controlo para os responsáveis pelo tratamento no que concerne aos atos automatizados, total ou parcialmente, e à obrigação de elaboração de registos de atividades de tratamento. Os responsáveis pelo tratamento passaram a assumir mais obrigações e responsabilidades no tratamento dos dados pessoais, mas ao mesmo tempo ganharam mais autonomia na tomada de decisões quanto à prática de atos durante o exercício das suas funções. Contudo com o desenrolar da aplicabilidade do RGPD foram sendo colocadas questões sobre se na realidade não estaremos perante uma heterorregulação mitigada ao invés

¹³¹ O artigo 21.º da Diretiva 95/46/CE estabelecia que eram as autoridades de controlo de cada Estado-Membro que tinham de ter um registo de acordo com o artigo 19.º da Diretiva.

de uma autorregulação, ou seja, se a autonomia acabada de referir na verdade apenas ocorre para uma parte dos atos praticados pelo responsável pelo tratamento.

Nos dias de hoje vemos que há por parte das empresas o recurso a diferentes softwares que permitem a execução, como vimos, de diferentes atos e funcionalidades que antes não existiam e que vieram permitir que a digitalização pudesse ocorrer e todos nós beneficiássemos com esta nova realidade. Os EUA são um dos principais criadores destes sistemas informáticos e consequentemente ao serem utilizados na União Europeia implicam que haja uma transferência de dados para um país que não se encontra no âmbito territorial de aplicabilidade do RGPD previsto no seu artigo 3.º. Havendo a necessidade de haver esta transferência é exigível que sejam elaborados acordos¹³² entre a UE e esses países, sob a coordenação e aprovação da Comissão Europeia, de modo a que seja acordado por parte destes países o cumprimento das normas europeias quanto ao tratamento de dados ou uma autorização por parte das autoridades de controlo nacionais. Há deste modo uma diminuição dos riscos que a transferência de dados¹³³ implica e uma consagração e garantia que há uma proteção adequada que irá ser praticada relativamente aos dados que lhe forem partilhados. Seria no mínimo contraditório considerar-se que as normas do RGPD têm que ser cumpridas e ao mesmo tempo permitir-se que haja uma facilidade na transferência de dados que põe em causa a segurança dos dados e a sua proteção¹³⁴. Estaríamos a exigir aos responsáveis pelo tratamento europeus por um lado, e a permitir por outro lado aos não europeus a possibilidade de agirem de acordo com níveis de exigência diferentes. A digitalização e as vantagens que podem ser conquistadas com ela não podem nunca se sobrepor aos riscos que com ela podem ocorrer e levar assim a que as desvantagens se sobreponham às vantagens.

Nos casos em que há acordos estabelecidos, não existe, nos termos do artigo 45.º, a necessidade de haver uma autorização específica sobre o tratamento de dados por parte das autoridades de controlo nacionais antes de a transferência de dados ocorrer. Neste caso haveria uma intervenção necessária de uma autoridade de controlo nacional antes que pudesse haver por parte do responsável pelo tratamento o início da atividade de tratamento, de modo a que

¹³² Já existem a nível das redes sociais acordos que permitem que haja um ponto de concordância sobre parâmetros de proteção e tratamento de dados a ser adotados pelos sistemas americanos e acautelam os dados na mesma medida e com o mesmo rigor que o RGPD entende.

¹³³ Estamos perante uma transferência de dados quando os dados são partilhados para um país terceiro ou para uma organização internacional à qual não se aplica o RGPD, mas com o qual pode ser celebrado acordos que permitem que haja um ponto comum de acordo quanto ao tratamento de dados.

¹³⁴ Comissão Europeia, "Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Explanatory Memorandum", 15 de outubro de 1992, p. 34, disponível em <http://aei.pitt.edu/10375/1/10375.pdf>, consultado no dia 30 de setembro de 2018.

fosse avaliada a salvaguarda dos dados pessoais. Mas havendo cada vez mais uma comunicação com outros mercados que não o nosso europeu e sendo necessário que assim o seja¹³⁵, podemos questionar se a vida económica não nos obrigou a ter que transferir dados para fora da União numa proporção superior à que seria esperada e se na verdade o que seria uma autorregulação dos dados se revelou na prática uma heterorregulação. Os responsáveis pelo tratamento continuam a ter a responsabilidade de tomar as decisões quanto aos atos que praticam, automatizados ou não, mas a verdade é que continuam a depender que haja uma regulação por parte da autoridade de controlo ou por parte da Comissão Europeia. Não há uma quebra de quem assume a decisão pelas atividades de tratamento que pretende desempenhar como parecia transparecer em 2016 com o regulamento face ao estabelecido em 1995 com a diretiva. Se para adotarmos um determinado sistema informático que implica uma transferência de dados temos que recorrer a mecanismos de avaliação da segurança dos dados quer através de uma autorização, no caso de não haver um acordo estabelecido naquela matéria, quer através de um prévio acordo, então estaremos perante uma necessidade que já existia antes e que continua atualmente. Um responsável pelo tratamento precisa que haja um acordo estabelecido ou a estabelecer ou de uma autorização para que possa exercer uma determinada atividade de tratamento relativamente a atos que existem na sua maioria hoje em dia como foi mencionado.

Esta autorização é dada através de uma decisão da Comissão, nos termos do artigo 45.º, depois de avaliados os riscos e percebido de que modo o país ou instituição que recebe os dados os trata e se existe uma adequação do tratamento dos dados ao caso em concreto. Esta avaliação é contínua, ou seja, tem que ser revista e reavaliada pela Comissão sempre que entender que seja necessário, podendo levar a uma mudança da decisão de existência do acordo caso haja alguma alteração ao tratamento executado que signifique uma desproteção dos dados. O receio que existe quanto ao tratamento de dados por entidades que não tenham na sua base as mesmas normas que a regulamentação europeia é a motivação de todas as revisões e ponderações que tem que ser feitas por parte da Comissão. É neste sentido necessário ter conhecimento de todas as listas de entidades, organizações ou instituições internacionais que já obtiveram aprovação no seu tratamento de dados e nesse sentido, apesar de haver ainda os riscos e não deixar de ser uma transferência de dados internacionais, não precisam de ser

¹³⁵ No Acórdão com o processo n.º C-362/14 no ponto 56 é mencionada esta dependência que existe em se apostar numa economia europeia capaz de se relacionar com outras economias e como essa capacidade é necessária para que se alcance uma evolução que se espera que aconteça e que seja o futuro da Europa.

autorizadas as atividades de tratamento nestes casos. Relativamente aos EUA¹³⁶¹³⁷, existe uma ligação estabelecida com a União Europeia, Inglaterra e Suíça que permite que haja um conhecimento do que é necessário para que haja o recurso a softwares americanos, existindo uma lista destes casos, o que ajuda significativamente dada a influencia e existência nestes softwares¹³⁸.

Há uma mitigação da realidade da responsabilidade quanto a quem determina que atividades ou atos podem ser praticados pelo responsável pelo tratamento sem precisar de terceiros para avaliar as suas decisões. Quando analisamos o regulamento percebemos que a aclamada autorregulação na verdade não existe na totalidade dos casos concretos ou podemos arriscar na maioria dos casos. Levanta-se a questão de como é que se soluciona os casos em que aparentemente não existe nenhuma divergência de aplicabilidade das normas e de quem assume a responsabilidade, mas na verdade ao analisarmos as atividades de tratamento ao pormenor e verificarmos que existe mais do que um meio automatizado podemos perceber que apesar de o responsável pelo tratamento ter adotado todas as medidas técnicas e organizativas que considerou como aplicáveis na verdade existe uma determinada atividade ou ato que não cumpriu a legislação europeia por falta de autorização ou acordo. Caso ocorra uma violação de dados podemos considerar que o princípio da segurança não foi cumprido pelo incumprimento do descrito apesar de haver um modelo de autorregulação imposto.

Na Administração Pública todos os tratamentos de dados nos serviços públicos têm que¹³⁹ cumprir sempre os princípios do artigo 5.º do RGPD, ter uma finalidade ou finalidades estabelecidas segundo o artigo 6.º do RGPD e cumprir a previsão do modo como os titulares podem exercer os seus direitos de acordo com o previsto nos artigos 12.º a 14.º sempre que recorrem a meios informáticos que levem a uma partilha de dados com outro serviço público seja de que nacionalidade for¹⁴⁰. Neste sentido também eles quando recorrem a sistemas informáticos que não aplicam o RGPD tem que garantir que existe um acordo com país que criou

¹³⁶ Podem ser consultadas mais informações em <https://www.dataprivacyframework.gov/>.

¹³⁷ Um dos casos em que foi colocada em causa a transferência de dados pessoais para os Estados Unidos ao se questionar a adequação no tratamento de dados foi o caso de SCHERMS. Este caso veio levantar questões sobre o cumprimento por parte dos EUA das normas que são identificadas na União Europeia como as protetoras do direito previsto no artigo 8.º do CDFUE e levar a que haja uma ponderação entre a existência de um ponto em comum criado para que haja um acordo de como o tratamento deve ocorrer e como este de facto ocorre. Esse caso é o caso mais mediático em matéria de transferência de dados pessoais e que merece o destaque pelas inquietações que veio provocar quanto à veracidade prática do acordo celebrado.

¹³⁸ <https://www.dataprivacyframework.gov/list>.

¹³⁹ O [Data Sharing and Governance Act 2019, Section 1 \(irishstatutebook.ie\)](#) refere que requisitos tem que ser cumpridos na partilha de dados entre serviços públicos. Apesar de ter sido criada pela Irlanda reflete a preocupação que os Estados Europeus devem ter no tratamento de dados nos serviços públicos.

¹⁴⁰ Esta maior exigência foi mencionada no Acórdão Bara & Others (C-201/2014) e demonstrou que o setor público tem características que o diferenciam do setor privado e que impõe que haja uma proteção que vá nesse sentido.

esses sistemas de modo a que haja uma proteção dos cidadãos e a consideração de que sendo uma entidade do setor público a quantidade de dados partilhados é superior assim como a responsabilidade que a mesma acarreta. Há como que uma maior exigência por parte dos cidadãos quanto aos serviços públicos. O mapa que se cria com a circulação de dados partilhados entre os serviços públicos e com os programas que são utilizados cria aqui uma problemática que leva a que haja uma delimitação clara de como os atos administrativos automatizados podem ser praticados e que pode levar a que esta heterorregulação mitigada que existe na prática derivada da previsão das normas de autorregulação do RGPD possa ser uma limitação à celeridade que se pretendia com a mudança de perspetiva com o regulamento.

Na Administração Pública foram criados os atos administrativos automatizados, que existem quando são praticados completamente ou parcialmente de forma eletrónica, que vieram desafiar o modo como aplicamos o direito administrativo e questionar como é que esta nova realidade deve ser entendida. Estes atos são praticados desde o seu início até ao fim por uma máquina, programada por seres humanos é certo, que decidirá e praticará o ato que considerar aplicável ao caso de acordo com o que foi programado por seres humanos. O ato administrativo que conhecemos deixa de existir em determinadas matérias e leva a que haja um entendimento diferenciado sobre que leitura e interpretação devemos ter sobre o modo como os serviços públicos se posicionam na vida dos cidadãos. Vem significar benefícios para os cidadãos e levar a que tenhamos serviços públicos e uma justiça com uma maior capacidade de resposta, mas levanta também questões sobre a capacidade de resposta para as entidades públicas se continuarem a ter uma dependência em autorizações ou acordos e deste modo a responsabilidade assumida pelo responsável.

Fica claro que nos casos em que se aplica o artigo 45.º do RGPD estamos perante uma heterorregulação feita pela Comissão prevista no sistema de autorregulação do RGPD. Não restam dúvidas que apesar de este diploma consagrar que quem assume a responsabilidade pelo tratamento de dados é o responsável pelo tratamento, não dependendo de nenhuma autorização ou controlo por parte da autoridade de controlo, mas, contudo, ao mesmo tempo, prevê que existem casos em que esta responsabilidade é assumida pelo responsável pelo tratamento mas com a intervenção e controlo da Comissão. Há como uma mitigação de uma realidade de prévia revisão e aprovação dos atos praticados pelo responsável pelo tratamento quando são utilizados meios automatizados, total ou parcialmente, e que fica de certo modo

disfarçada pelas normas previstas no RGPD. Pode ser argumentado que apenas em determinados casos é que há uma intervenção da Comissão, mas rapidamente se percebe que com o mundo tecnológico como temos o de hoje e com a quantidade de dados que circulam a probabilidade de haver uma necessidade de controlo prévio é demasiado elevada para que consideremos que a autorregulação se sobrepõe à heterorregulação que tem que existir de acordo com as normas do RGPD. Como vimos anteriormente mesmo havendo um acordo celebrado, não significa que não tenha de haver um controlo da aplicabilidade e adequação para a realidade que foi criado.

O cumprimento das medidas técnicas e organizativas, na decorrência do princípio da segurança, e a necessidade de haver um controlo prévio de atos que podem implicar um maior risco para os dados pessoais dos titulares dos dados, com a transferência internacional de dados, tem como objetivo um tratamento de dados direcionado para a tutela dos dados pessoais dos titulares dos dados que confiaram ao responsável pelo tratamento. O responsável pelo tratamento dos dados tem que ter a consciência de que o titular dos dados tem direito a toda a transparência sobre como os dados que lhe confiou estão a ser tratados, em cumprimento do princípio da lealdade. Não revela para ele quem é que vai controlar os atos praticados pelo responsável pelo tratamento. A lei tem que se necessário que esteja tudo esclarecido e determinado legalmente de quem é que verdadeiramente assume a determinação de quais os atos que podem para que saibam os responsáveis pelo tratamento e as autoridades nacionais como agir.

Conclusão

A presente dissertação de mestrado, neste tema tão atual como é a adoção de meios tecnológicos na sociedade, permitiu concluir que um longo caminho tem sido percorrido quanto ao papel da tecnologia na sociedade e no direito e que está longe de estar concluído. Um caminho complicado, com desafios, mas que se tem revelado gratificante e de reconhecido valor para os Estados e seus cidadãos ao permitir que haja um desenvolvimento de soluções que correspondam às necessidades individuais e coletivas de uma sociedade. Em termos legislativos revelou-se importante a criação de instrumentos que estabelecessem conceitos, delimitassem limites e obrigações ao tratamento de dados e estabelecessem quem assumiria a responsabilidade em caso de desrespeito pelas normas previstas em diversos diplomas sobre a aplicação de meios tecnológicos. A adoção de meios tecnológicos não era o principal problema, mas sim a percepção de como haveria a criação de uma realidade diferente, e com proporções que rapidamente se revelariam de resolução complicada, ser tratada de modo a que a proteção de dados fosse sempre a prioridade.

A questão que verdadeiramente se coloca nesta matéria é a clareza na definição de responsabilidade em caso de violação de dados. Se os dados forem partilhados indevidamente ou utilizados para finalidades não consentidas pelo titular dos dados tem que haver uma definição de quem assumirá em todos esses casos, de forma expressa ou por analogia, a responsabilidade. Esta começa a ser definida desde o início da prática dos atos, ou seja, desde o momento em que o responsável pelo tratamento de dados decide praticar determinado ato que envolve dados pessoais e apenas termina quando a(s) finalidade(s) para as quais foram partilhados os dados deixaram de existir ou no caso de o consentimento for retirado pelo titular dos dados.

No caso da Administração Pública a decisão de uma entidade pública começar a praticar determinado ato tem que decorrer de uma prévia definição de quem irá controlar a sua legalidade quanto ao tratamento e proteção de dados pessoais. Inicialmente nos primeiros diplomas foi definido a heterorregulação em que seria da responsabilidade da autoridade nacional da proteção de dados, a CNPD, o controlo e decisão sobre todos os atos, não havendo a responsabilidade do responsável pelo tratamento de dados, que se queriam praticar e que envolvessem dados pessoais. Rapidamente se percebeu que se queríamos avançar nesta matéria não poderíamos depender todas as decisões numa única autoridade/entidade. A demora e a sobrecarga que existiam excluía qualquer praticabilidade que se pudesse querer numa matéria que se queria

com a capacidade de resposta adequada à velocidade de desenvolvimento da matéria. Concluiu-se que essa responsabilidade teria de caber ao responsável pelo tratamento e que à autoridade apenas caberia um controlo à posteriori, passando de uma heterorregulação para uma autorregulação. A realidade tem revelado que esta mudança da “titularidade” da responsabilidade tem tido pouca aplicação na prática devido ao que a direito sempre nos habituou: para toda a regra há uma exceção. As diversas exceções e a sua aplicação recorrente nos casos concretos fazem levantar a questão se não estamos perante não de uma autorregulação, mas sim de uma heterorregulação mitigada. Perspetiva-se a necessidade de uma nova mudança no modo de definição de responsabilidade e de um maior reconhecimento de capacidade de os responsáveis pelo tratamento na definição de quais os atos que irão representar um impacto negativo nos dados pessoais superior às vantagens que deles derivariam.

Lista Bibliográfica

ABREU, Joana Covelo de “Os princípios gerais da Administração Pública em linha na União Europeia e a análise do artigo 14.º do CPA – revisitando as necessidades de literacia digital” in Carla Amado Gomes *et al.* (ed.), *Comentários ao Código do Procedimento Administrativo*, Lisboa, AAFDL, volume I, 2023.

ALVES, Joel A. – “Administração eletrónica, eficiência e proteção de dados: breves considerações à luz dos princípios gerais da atividade administrativa”, in PEREIRA COUTINHO, Francisco e CANTO MONIZ, Graça (coord.). *Anuário da Proteção de Dados 2022*. Lisboa: CEDIS, 2022.

ALVES, Joel A. – *O novo modelo de proteção de dados de dados pessoais europeu*, Coimbra, Almedina, 2021.

BRANDÃO, Ana Paula *et al.* (eds.) - *Enciclopédia da União Europeia*, Lisboa, Petrony, 2017.

CALVÃO, Filipa Urbano – “Os estados de exceção e a proteção de dados pessoais”, in Carla Amado Gomes *et al.* (ed.), *Direito Administrativo de necessidade e de exceção*, Lisboa, AAFDL Editora, 2020.

CORDEIRO, A. Barreto Menezes, - *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*, Coimbra, Almedina, 2021.

CORDEIRO, A. Barreto Menezes, “Direito de Proteção de Dados”, Almedina, Coimbra, 2022

COUTINHO, Francisco Pereira, “A independência da Comissão Nacional de Proteção de Dados”, in Francisco Pereira Coutinho *et al.* (ed.), *Anuário da Proteção de Dados*, Lisboa, CEDIS, 2020.

DELGADO, Isaac Martín, “El acceso electrónico a los servicios públicos: hacia um modelo de administración digital autenticamente inovador”, in *Sociedad Digital y Derecho*, Imprensa Nacional del Boletín Oficial del Estado, 2018.

FONSECA, Isabel Celeste, “Governança Pública (Local) Digital: notas breves sobre a estratégia em curso de aceleração da transição digital”, in Artur Flaminio da Silva (coord.), *Direito Administrativo e Tecnologia*, Coimbra, Almedina, 2021.

FREITAS, Tiago Fidalgo de *et al.* (eds.) - *Direito da Proteção de Dados: perspetivas públicas e privadas*, Coimbra, Almedina, 2023.

FREITAS, Tiago Fidalgo, e ALVES, Pedro Delgado – *O acesso à informação administrativa*, 1ª Edição, Almedina, 2021.

MAGALHÃES, Filipa Matias, e PEREIRA, Maria Leitão – *Regulamento Geral de Proteção de Dados - Manual Prático*, Porto, VidaEconómica, 2017.

MONIZ, Graça Canto – *Manual de Introdução à Proteção de Dados Pessoais*, Coimbra, Almedina, 2023.

RODRIGUES, José Noronha, e TEVES, Daniela Medeiros – *A proteção de dados pessoais e a Administração Pública – O novo paradigma jurídico*, Lisboa, AAFDL Editora, 2020.

SALDANHA, Nuno – *Novo Regulamento Geral de Proteção de Dados - O que é? A quem se aplica? Como implementar?*, Lisboa, FCA, 2020.

SANTOS, Graça - *O Regulamento Geral de Proteção de Dados da Teoria à Prática*, Lisboa, Chiado Editorial, 2023.

SANTOS, Helena Patrícia Neves dos, “Administração eletrónica local: análise sobre a modernização da administração local e respetivos desafios”, in Isabel Celeste M. Fonseca (dir.), *Governança Pública Digital, Smart Cities e Privacidade*, 1ª Edição, Coimbra, Almedina, 2022.

SANTOS, Sofia Berberan, e GABRIEL, João, “Regulamento Geral sobre a Proteção de Dados, Legislação e Algumas Notas”, Lisboa, Edição GPA Academy, 2020.

SILVA, Artur Flaminio, “Inteligência Artificial e Direito Administrativo”, in Artur Flaminio Silva (dir.), *Direito Administrativo e Tecnologia*, 2ª Edição, Coimbra, Almedina, 2021.

Bibliografia Eletrónica

<http://aei.pitt.edu/10375/1/10375.pdf>.

<https://americaninnovators.com/digitaltransformation/>.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digitalage/shaping-europes-digital-future_pt.

<https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance>.

<https://digital-strategy.ec.europa.eu/en/policies/desi>.

<https://digital-strategy.ec.europa.eu/en/policies/desi-portugal>.

<https://www.portugal.gov.pt/pt/gc22/comunicacao/noticia?i=governo-aprova-estrategia-para-a-transformacao-digital-da-administracao-publica-2021-2026>.

<https://digital-strategy.ec.europa.eu/en/policies/egovernment>.

https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

<https://edpb.europa.eu/system/files/2022->

02/eppb_guidelines_202007_controllerprocessor_final_pt.pdf.

<https://eurocid.mne.gov.pt/europa-digital>.

<https://joinup.ec.europa.eu/>.

https://knowledge4policy.ec.europa.eu/foresight/digital-transformation-public-administration-services_en.

https://repositorium.sdum.uminho.pt/bitstream/1822/71364/1/relatorio_etica.direito2020_observatoriociberseguranca_cnccs.pdf.

<https://tic.gov.pt/documents/37177/280325/Plano+de+A%C3%A7%C3%A3o+Transversal+para+a+Transforma%C3%A7%C3%A3o+Digital+da+AP+2021-2023.pdf/1a8bdefc-ad29-e7a9-898c-d21f55cbea7b>.

<https://www.cada.pt/files/pareceres/2022/277.pdf>.

https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf.

<https://www.dataprivacyframework.gov/>.

<https://www.dataprivacyframework.gov/list>.

https://www.edps.europa.eu/sites/default/files/publication/brochure_2009_pt.pdf.

https://www.europarl.europa.eu/pdfs/news/expert/2021/4/story/20210414STO02010/20210414STO02010_pt.pdf.

<https://www.irishstatutebook.ie/eli/2019/act/5/section/1/enacted/en/html>.

<https://www.simplex.gov.pt/>.

Legislação, Diretrizes e Pareceres

- Código Civil – disponível em

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis.

- Código do Procedimento Administrativo – disponível em

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2248&tabela=leis.

- Constituição da República Portuguesa disponível em

<https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>.

- Diretiva 95/45/CE – disponível em <https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>.

- Lei n.º 67/98, de 26 de outubro disponível em

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=156&tabela=leis.

- Lei n.º 26/2016, de 22 de Agosto – disponível em

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2591A0009&nid=2591&tabela=leis&ficha=1&nversao=.

- Lei da Proteção de Dados Pessoais – disponível em

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3118&tabela=leis&nversao=.

- REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) – disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1667850894976&from=PT>.

- REGULAMENTO (UE) 2018/1725 DO PARLAMENTO EUROPEU E DO CONSELHO de 23 de outubro de 2018 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE – disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R1725>.

- Diretrizes 05/2020 disponível em

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf.

- Parecer n.º: 1 de 16/01/1997 - [Processo(s) n.º: 169] disponível em <https://www.cada.pt/files/pareceres/1997/001.pdf>.

- Parecer n.º 277/2022 com o Processo n.º 360/2022 disponível em <https://www.cada.pt/files/pareceres/2022/360.pdf>.

Jurisprudência

Tribunal de Justiça da União Europeia:

- Acórdão com o processo n.º C-614/10 de 16 de outubro de 2012;
- Acórdão com o processo n.º C-293/12 de 8 de abril de 2014;
- Acórdão com o processo n.º C-131/12 de 13 de maio de 2014;
- Acórdão com o processo n.º C-201/2014 de 1 de outubro de 2015;
- Acórdão com o processo n.º C-362/14 de 6 de outubro de 2015;
- Acórdão com o processo n.º C-434/16 de 20 de dezembro de 2017.

Supremo Tribunal Administrativo:

- Acórdão com o processo n.º 0169/10 de 12 de maio de 2010;
- Acórdão com o processo n.º 0684/21.6BELSB de 3 de novembro de 2022.

Tribunal da Relação de Lisboa:

- Acórdão com o processo n.º 842/16.5T8ALQ.L1-3 de 17 de maio de 2017.